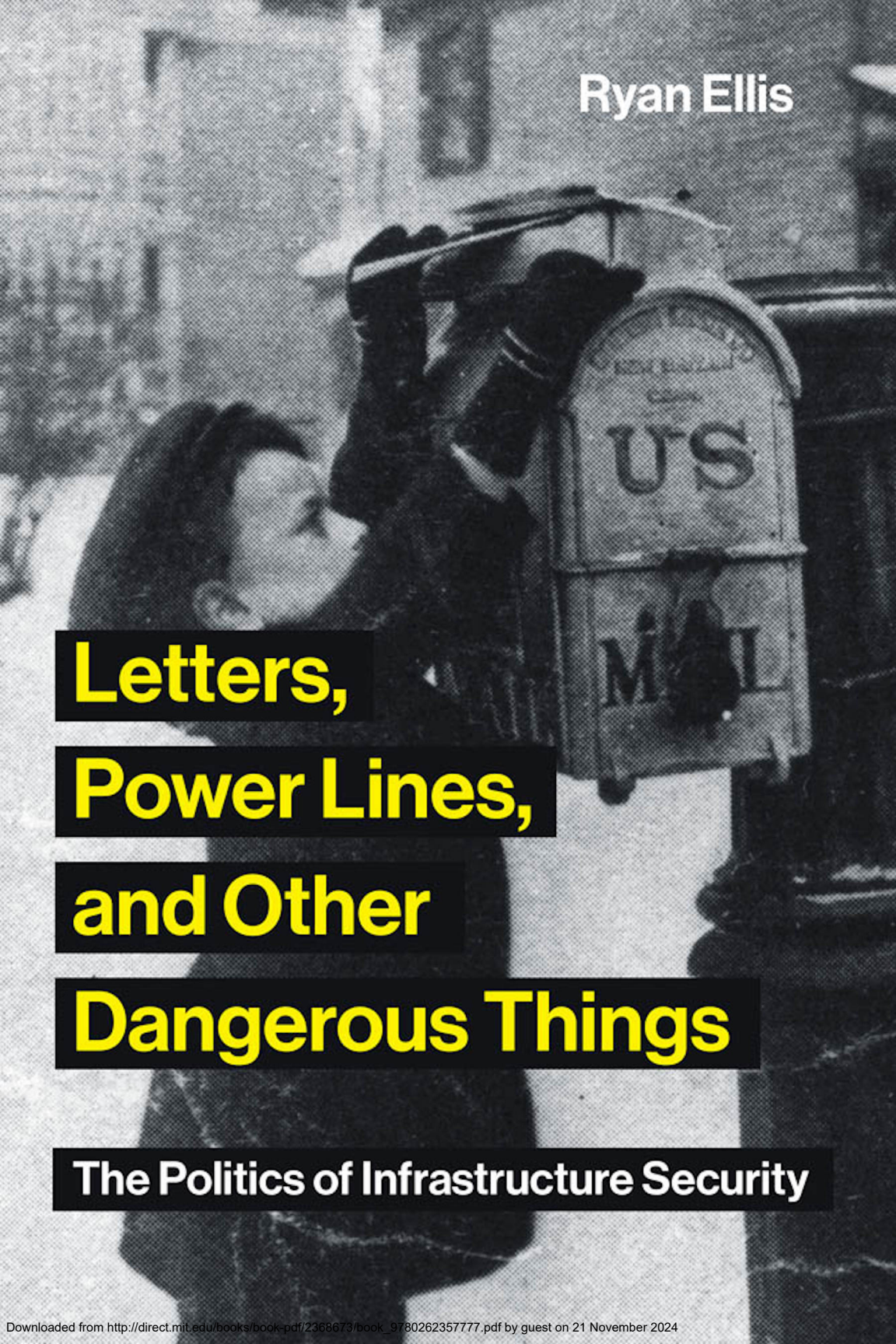


Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Letters, Power Lines, and Other Dangerous Things

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Infrastructures Series

edited by Geoffrey C. Bowker and Paul N. Edwards

Paul N. Edwards, *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*

Lawrence M. Busch, *Standards: Recipes for Reality*

Lisa Gitelman, ed., *"Raw Data" Is an Oxymoron*

Finn Brunton, *Spam: A Shadow History of the Internet*

Nil Disco and Eda Kranakis, eds., *Cosmopolitan Commons: Sharing Resources and Risks across Borders*

Casper Bruun Jensen and Brit Ross Winthereik, *Monitoring Movements in Development Aid: Recursive Partnerships and Infrastructures*

James Leach and Lee Wilson, eds., *Subversion, Conversion, Development: Cross-Cultural Knowledge Exchange and the Politics of Design*

Olga Kuchinskaya, *The Politics of Invisibility: Public Knowledge about Radiation Health Effects after Chernobyl*

Ashley Carse, *Beyond the Big Ditch: Politics, Ecology, and Infrastructure at the Panama Canal*

Alexander Klose, translated by Charles Marcrum II, *The Container Principle: How a Box Changes the Way We Think*

Eric T. Meyer and Ralph Schroeder, *Knowledge Machines: Digital Transformations of the Sciences and Humanities*

Sebastián Ureta, *Assembling Policy: Transantiago, Human Devices, and the Dream of a World-Class Society*

Geoffrey C. Bowker, Stefan Timmermans, Adele E. Clarke, and Ellen Balka, eds., *Boundary Objects and Beyond: Working with Leigh Star*

Clifford Siskin, *System: The Shaping of Modern Knowledge*

Lawrence Busch, *Knowledge for Sale: The Neoliberal Takeover of Higher Education*

Bill Maurer and Lana Swartz, *Paid: Tales of Dongles, Checks, and Other Money Stuff*

Dietmar Offenhuber, *Waste Is Information: Infrastructure Legibility and Governance*

Katayoun Shafiee, *Machineries of Oil: An Infrastructural History of BP in Iran*

Megan Finn, *Documenting Aftermath: Information Infrastructures in the Wake of Disasters*

Laura Watts, *Energy at the End of the World: An Orkney Islands Saga*

Ann M. Pendleton-Jullian and John Seely Brown, *Design Unbound: Designing for Emergence in a White Water World*, Volume 1: *Designing for Emergence*

Ann M. Pendleton-Jullian and John Seely Brown, *Design Unbound: Designing for Emergence in a White Water World*, Volume 2: *Ecologies of Change*

Jordan Frith, *A Billion Little Pieces: RFID and Infrastructures of Identification*

Morgan G. Ames, *The Charisma Machine: The Life, Death, and Legacy of One Laptop per Child*

Mario Biagioli and Alexandra Lippman, eds., *Gaming the Metrics: Misconduct and Manipulation in Academic Research*

Malcolm McCullough, *Downtime on the Microgrid: Architecture, Electricity, and Smart City Islands*

Emmanuel Didier, translated by Priya Vari Sen, *America by the Numbers: Quantification, Democracy, and the Birth of National Statistics*

Ryan Ellis, *Letters, Power Lines, and Other Dangerous Things: The Politics of Infrastructure Security*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Letters, Power Lines, and Other Dangerous Things

The Politics of Infrastructure Security

Ryan Ellis

The MIT Press
Cambridge, Massachusetts
London, England

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

© 2020 Massachusetts Institute of Technology

This work is subject to a Creative Commons CC-BY-NC-ND license. Subject to such license, all rights are reserved.

The open access edition of this book was made possible by generous funding from Arcadia—a charitable fund of Lisbet Rausing and Peter Baldwin.

This book was set in Sabon by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data

Names: Ellis, Ryan, author.
Title: Letters, power lines, and other dangerous things : the politics of infrastructure security / Ryan Ellis.
Description: Cambridge, Massachusetts : The MIT Press, [2020] | Series: Infrastructures | Includes bibliographical references and index.
Identifiers: LCCN 2019025809 | ISBN 9780262538541 (paperback) | ISBN 9780262357777 (ebook)
Subjects: LCSH: Infrastructure (Economics)--United States--Security measures.
Classification: LCC HC110.C3 E456 2020 | DDC 363.11/93880973--dc23
LC record available at https://lccn.loc.gov/2019025809

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Contents

Acknowledgments vii

Introduction: Letters, Power Lines, and Other Dangerous Things 1

I The Political Origins of Infrastructure Vulnerability 29

1 Stumbling toward Resilience: The Overlooked Virtues of Regulation 31

2 The Political Origins of Infrastructure Vulnerability: The Hidden Vices of Deregulation 87

II Ubiquitous Targets: Infrastructure Security after September 11 137

3 Imagination Unbound: Risk, Politics, and Post-9/11 Anxiety 139

4 Infected Mail: Labor, Commerce, and the 2001 Anthrax Attacks 165

5 Green Security: The Environmental Movement, the Transportation of Hazardous Materials, and the War on Terror 185

6 Regulating Cybersecurity: The Unexpected Remaking of Electric Power 209

Conclusion: The Politics of Critical Infrastructure Protection 239

Coda: Infrastructure as Target 249

Notes 253
Bibliography 329
Index 353

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Acknowledgments

This book began with a snap. In 2003 I was working in a post office in Brookline, Massachusetts, as a letter carrier. During my first day on the job, I noticed another worker methodically putting on latex gloves before picking up the mail. *Snap*. A nearby coworker must have noticed my confusion. He leaned over and offered a tart explanation: *anthrax*. And then we all went about our day and delivered the mail. That morning offered a glimpse into how terrifying fears and moments of disruption become translated into routine practices. The anthrax attacks that had run through the postal system were, at this point, roughly 18 months in the past. Yet traces still lingered. That morning stuck with me. Although I did not know it at the time, this book started that day.

This project would not have been possible without the support and mentorship of a large number of people and institutions. This book began as my doctoral project at the Department of Communication at the University of California, San Diego (UCSD). My advisor and mentor Robert Horwitz is the inspiration for this book. I would not have been able to write it without his assistance, encouragement, and wisdom. Robert was my first and best reader. I owe him more than I can pay. While at UCSD I started working with Lewis Branscomb. Lew helped me rethink my doctoral project at a time when I was grasping for a direction. Lew continued to provide unfailing support as I left UCSD and began my academic journey. The text was substantially revised during fellowships at Stanford University's Center for International Security and Cooperation (CISAC) and the Harvard Kennedy School's Belfer Center for Science and International Affairs and at my current academic home, Northeastern University's Communication Studies Department. At Stanford I had the privilege of working closely with Charles Perrow. Perrow's work was and remains a key touchstone for my thinking. Getting to work with Chick was an honor and thrill that I cherish. His comments on the text

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

were invaluable. At Harvard, Venkatesh Narayanamurti provided a new intellectual role model and a welcome academic home. Venky's support helped this book become a reality. His constant push to consider all sides of an argument and never lose sight of the larger issues and stakes at play was an important guiding force. My colleagues at Northeastern have been inspiring. Keeping up with them is not an easy task.

During the preparation of this book, I received significant comments and feedback. I would like to thank Michael Schudson, Akos Rona-Tas, Gary Fields, Lynn Eden, Mariano-Florentino Cuéllar, Whitfield Diffie, Susan Landau, and Bruce Schneier for their comments on early drafts and chapters. My thinking on these topics has been significantly shaped by a number of current and former colleagues. I would like to particularly thank Joe Nye, Jim Waldo, Bill Hogan, Jack Goldsmith, Lucas Kello, Vivek Mohan, Zach Tumin, Benoit Gaucherin, Nazli Choucri, Fred Turner, John Downer, Rebecca Slayton, Ted Lewis, Rudy Darken, Thomas Mackin, J. R. Osborn, Lyn Headley, Stephen Flynn, and Jennie Stephens. Administrative support from Gayle Aruta, Jamie Llyod, Karin Vander Schaaf, Patricia McLaughlin, Sarah Donahue, and Angela Chin was indispensable. Early iterations of the arguments in this book were presented at the annual conferences of the Society for Social Studies of Science, the National Communication Association, the International Communication Association, and the Society for the History of Technology, as well as during presentations to the Harvard Electricity Policy Group and the National Association of Regulatory Utility Commissioners. The various participants at these discussions offered useful and challenging feedback. At MIT Press, Katie Helke extended a great deal of patience and expert editorial suggestions; Justin Kehoe offered timely advice and excellent assistance. Series editors Geoffrey Bowker and Paul Edwards provided sharp comments and feedback that made this book better. Various anonymous reviewers also provided insightful suggestions that were incorporated into the text. All errors and mistakes are my own.

An earlier version of chapter 4 appeared as "Creating a Secure Network: The 2001 Anthrax Attacks and the Transformation of Postal Security" in the *Sociological Review*. The short discussion of E-COM in chapter 2 is expanded in my earlier article "The Premature Death of Electronic Mail: The United States Postal Service's E-COM Program, 1978–1985" in the *International Journal of Communication*; a discussion of some of the governance issues noted in chapter 6 previously appeared in my article "Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?" in *IEEE Security & Privacy*.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

A number of awards supported various aspects of this work, including fellowships and grants from the University of California, San Diego; the Institute for Research on Labor and Employment at the University of California, Los Angeles; CISAC, Stanford University; the Belfer Center for Science and International Affairs, Harvard Kennedy School; and the Smithsonian National Postal Museum/National Philatelic Exhibitions of Washington, DC (NAPEX). Early-stage preparatory work was funded, in part, by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.

Finally, and most importantly, I would like to thank my family and friends. Their warmth, kindness, and love are deeply appreciated. Growing up in a lively and curious household was a gift. For that and much more, I have my parents and brother to thank. I dedicate this book to Erin, Veronica, and Indigo. Their support, encouragement, and love make this and everything else possible. Words cannot express how lucky and grateful I am.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Introduction

Letters, Power Lines, and Other Dangerous Things

On March 12, 2013, Director of National Intelligence (DNI) James Clapper publicly testified before the Senate Select Committee on Intelligence.[1] As DNI, Clapper sat atop the U.S. intelligence bureaucracy, coordinating and overseeing the efforts of 17 different intelligence agencies, bureaus, offices, and services, including the National Security Agency (NSA) and the Central Intelligence Agency (CIA). Clapper was plainly uncomfortable. A long-standing veteran of the intelligence world, Clapper could not help but note that "an open hearing on intelligence matters is something of a contradiction in terms."[2] Reading stiffly from prepared remarks, Clapper presented the 2013 *World Wide Threat Assessment*, an annual unclassified summary of the intelligence community's consensus assessment of threats to U.S. national security.[3] In an unprecedented and important symbolic move, the intelligence community listed threats—specifically cyber threats—to critical infrastructure networks first.[4] Threats targeting critical infrastructure ranked ahead of weapons of mass destruction, terrorism, and transnational crime.[5] The assessment revealed, in Clapper's words, "how quickly and radically our world—and our threat environment—are changing."[6] The nation's top spy might question the wisdom of public testimony, but he was nonetheless clear: infrastructure protection was emerging as *the* challenge of the 21st century.

Clapper's prioritization of the protection of critical infrastructure—systems that include telecommunications networks, the electric power grid, financial systems, transportation networks, and others that the federal government views as essential to the nation's security, health, and economic prosperity—is the culmination of a transformation in how policymakers and much of the public view infrastructures. In the years since the terrorist attacks of September 11, 2001, infrastructures have been recast as sites of anxiety and danger. The mundane systems that undergird much of modern life acquired a sinister tint: no longer were these networks

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

simply regarded as the boring background wiring of modern society; they were now *soft targets* that immediately required new, enhanced protections. In the weeks and months that followed 9/11, President George W. Bush made it clear that infrastructure security would be a key plank in a new, expansive homeland security agenda. In quick succession, a patchwork of new laws, policies, technologies, and practices focusing on infrastructure protection unspooled. In October 2001, Bush created the Office of Homeland Security within the executive branch and tasked it with coordinating federal infrastructure protection efforts. The Office of Homeland Security would, in a matter of mere months, be replaced by a vast newly created federal department: the Department of Homeland Security (DHS). The creation of DHS was a massive reorganization—the largest reshuffling of the federal government since the establishment of the Department of Defense in 1947.[7] Infrastructure protection sat at the center of DHS's new mandate. The primacy of infrastructure protection endured during the administration of President Obama and has showed no signs of waning during the Trump administration.[8]

The reframing of infrastructures as insecure spaces justified a significant and unprecedented investment in infrastructure security. It was a stunning transformation. For years a string of public commissions, policy reports, and little-read think-tank missives had warned that the nation's infrastructures were vulnerable to attack. Before 9/11 they tried, again and again, to push policy-makers and the public to prioritize infrastructure protection. Their warnings went largely ignored. In early 2001 the federal effort to protect critical infrastructure was being run from the Department of Commerce's Bureau of Export Administration by a tiny, obscure office—the Critical Infrastructure Assurance Office—with a modest annual budget of $5 million.[9] Across the entire federal government, critical infrastructure protection spending ranged from $1.1 billion to $2.7 billion annually between 1998 and fiscal year 2001.[10] Infrastructure protection was, at best, little more than an afterthought. Two decades later, the picture is radically different. Infrastructure protection is now a priority. By 2016 the federal government would devote a staggering sum—over $20 *billion*— to critical infrastructure protection annually.[11] DHS alone now receives over $5 billion annually to fund programs directly related to infrastructure protection. Across the federal government, roughly one-third of all homeland security spending is devoted to infrastructure protection.[12] If anything, these numbers significantly underreport government spending on infrastructure protection. They do not include state and local efforts, private-sector investment, or border and transportation

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

security—a distinct federal funding category currently divorced from critical infrastructure protection in public accounting. If border and transportation security are added to the mix, the figures begin to overwhelm: $51.5 billion in total federal funds—70% of federal homeland security funding—is devoted to protecting the nation's infrastructure.[13]

The influx of funding and attention has left its mark. The post-9/11 emphasis on infrastructure protection has remade the material and organizational foundations of infrastructures. Some of these new interventions are obvious and hard to miss. Barricades, bollards, and large, ugly concrete "security planters"—oversized flowerpots designed to thwart cars and vans from ramming into buildings, mowing down pedestrians, or delivering a deadly explosion—dot busy city streets and public squares.[14] Boarding a commercial flight heading from Boston to San Francisco now requires a familiar post-9/11 ritual: shoes, belt, and coat slipped off; shampoo, conditioner, and all other liquids stored in clear ziplock bags; laptop removed from the backpack and placed (always alone, never with shoes or coat) in a plastic bin for x-ray; arms raised as you stand inside an advanced imaging technology (AIT) body scanner for inspection; and then waiting until the Transportation Security Administration (TSA) agent tells you to collect your things and continue on your way, a few steps closer to your flight and to San Francisco.[15] Symbols of post-9/11 infrastructure anxiety are everywhere. Posters and signs plastered in train stations and subways running underneath New York City proclaim what the *Washington Post* describes as the nation's unofficial motto of post-9/11 life: *If you see something, say something*.[16] Dreamed up by a New York advertising executive on September 12, 2001, the slogan has become a marker of a transformed landscape: riding subways and trains now requires constant vigilance. Infrastructures are not just the foundations of contemporary life: they are fragile targets in waiting.[17]

Other infrastructural changes and alterations are subtle and can be difficult to see. Inside post offices across the U.S., detection and tracking systems developed by the defense contractor Northrop Grumman now test millions of letters for hints of a possible biological attack as they whirl through the postal network each day.[18] New security practices reach deep into the "guts" of infrastructure. Verizon, AT&T, and other commercial Internet service providers (ISPs) use classified information provided by DHS to scan data flowing over their commercial networks for signs of malicious traffic.[19] New security regulations require workers at the nation's ports to submit fingerprints and undergo a "security threat assessment" in order to receive a Transportation Worker Identification

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Credential (TWIC) from the TSA before accessing ports and vessels.[20] These changes may not be obvious to the public. For those of us outside of these infrastructures, they can be easy to miss. But, they matter: new security practices are remaking infrastructures in ways that will endure for decades (or longer). These changes may first be introduced during a moment of fresh panic, but once in place they become encased in custom and habit. In time, what was novel becomes simply "the way things are done": security practices become entrenched as part of the sunk politics of infrastructure that is taken for granted as normal and dull.

Behind the web of new security policies, laws, and embedded technologies that oversee infrastructure sits a larger long-running battle over infrastructural control. Infrastructures are systems that support *other* forms of activity. When they work well, we hardly notice them. As Paul Edwards observes, these systems become taken for granted, part of the "naturalized background, as ordinary and unremarkable as trees, daylight, and dirt."[21] Infrastructures are, to be sure, platforms. They are the foundations upon which other forms of activity rest. But they are not, nor have they ever been, *neutral* platforms.[22] The terms upon which they operate matter: infrastructures organize users, owners, regulators, workers, and uses in particular relationships that benefit and recognize some at the expense of others. From the moment they are created until the moment they are discarded, abandoned, and left to rot, infrastructures are sites of conflict over the terms of these relationships. These skirmishes often occur mostly offstage, buried within technical reports, arcane debates about cost allocation methodologies, and little-attended public hearings on zoning ordinances. Occasionally, however, infrastructures are inverted: the systems that sit in the background are briefly thrust into the foreground. These are key moments. For a fleeting instant, infrastructures are made visible and open to significant change. The political choices—power—inscribed within their operation become bald. The aftermath of 9/11 was one such moment. Infrastructures were now suddenly visible and open to renegotiation. The stakes were high. The administration of President George W. Bush might have made infrastructure protection a priority, but it left much of the details about how these vast networks and systems would actually be secured or protected unclear—the details would be worked out in the years to come. A cross section of actors and coalitions clashed and fought for control. New forms of security held out the real possibility of reshuffling how infrastructures are organized: Which sorts of users would be favored under new security guidelines? What type of uses would be deemed risky? Who would have a voice in crafting new security

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

protocols—workers, local politicians, industry? New security practices threatened to scramble how infrastructures operate and are organized; they held the potential to upend these sociotechnical systems in ways that might intensify or reverse the currents of power and control for years to come. In making sense of new forms of security, then, it is important to ask not only whether new security practices "work" but also "For whom do they work?" and "What type of social relations do they produce?"[23] These and other questions hung in the air during the first two decades of the 21st century as protecting infrastructure moved from being an idle and somewhat esoteric concern to an imperative.

* * * *

Letters, Power Lines, and Other Dangerous Things tries to make sense of the disorienting and contradictory infrastructural changes that have unfolded since September 11. It uncovers how the threat of terrorism is etched into the inner workings of infrastructures through new laws, regulations, technologies, and practices. The book maps these changes—why they happened, why they matter, and how they fit into the larger mosaic of both infrastructure governance and post-9/11 politics—through an examination of three U.S. infrastructures: the postal system, the freight rail network, and the electric power system. Each of these infrastructures underwent significant post-9/11 security overhauls. Cracking open the "black box" of infrastructure security practices reveals pointed conflicts, constitutive choices, and the accumulation of crosscutting forces that otherwise remain out of view. Rich and important stories emerge. Behind new forms of postal security sits a pitched, decades-long battle among unionized postal workers, key large-volume mailers, and postal management for control of the postal bureaucracy. Debates about how to protect against biological hazards—namely, anthrax—sent through the mail spiraled into larger arguments about the balance between workers' rights, the power of commercial, so-called junk mailers, and the shifting fortunes of old media in a new media world. New post-9/11 controls over rail shipments of toxic materials reveal how the rise of the "war on terror" enabled environmental activists to build a powerful coalition of activists, city and state officials, and members of Congress to take on the rail industry and the influential chemical lobby. A close look at the history of the first mandatory cybersecurity standards for the electric power industry illuminates how otherwise marginal federal regulators maneuvered to transform what appeared to be thin administrative powers into a robust system of accountability. These and other stories are written in the new

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

security standards, regulations, and technologies embroidered within these larger networks.

This book casts post-9/11 infrastructure security efforts in a new light. It finds within contemporary infrastructure security practices attempts to create new forms of *public accountability*. In the three cases examined, new security interventions made or sought to make infrastructures open to the concerns and interests of different groups—*infrastructure publics*—that are defined through their connection to the larger system.[24] This opening, and attempted opening, of infrastructures to plural publics and competing logics was significant. In the decades before 9/11, political and economic restructuring pushed infrastructure governance increasingly out of the public's reach. Years of market-based restructuring elevated infrastructure owners and operators—and some particular customers—into positions of unrivaled power. These same changes in political economy also altered the material organization of these systems in ways that made them increasingly vulnerable to large-scale failures. In the three cases examined, post-9/11 reforms attempted to wrestle back public control and address the vulnerabilities that now pocked these systems. In an odd twist, the vernacular of the war on terrorism offered otherwise marginalized groups the opportunity to have their voices heard and supported the creation of new political coalitions that agitated for greater public supervision over infrastructure. The threat of terrorism was a useful and powerful political resource. New forms of infrastructure security attempted to address the vulnerabilities caused by market-based reforms and, at the same time, reassert a degree of public control—control characterized by a recognition of the different publics and values present—over infrastructure. These efforts were not always successful—postal reforms initially held out the promise of offering postal workers a greater stake in making major decisions about how the postal network would operate and evolve, but these hopes were short-lived as key players (large-volume commercial mailers) outmaneuvered the postal unions and reasserted and strengthened their grip on postal policy. But in both electric power and freight rail, concerns over terrorism and security provided the foundation for new, durable forms of public accountability.

This portrait complicates conventional accounts of post-9/11 infrastructure security. Critical appraisals of post-9/11 infrastructure security typically paint a decidedly bleak picture. Often, infrastructure security is seen as little more than "security theater": ritual displays that do little to actually enhance security while, at best, offering some psychological benefits.[25] Asking passengers to take off their shoes before boarding an

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

airplane might do little to improve security, the thinking goes, but this bit of theater might make passengers feel safer. Elsewhere, contemporary infrastructure security efforts are taken to be a pretext for the troubling consolidation of power.[26] In this view, infrastructure security looks like an unholy alliance between corporate players and the state—what the author Naomi Klein describes as *disaster capitalism*. In this telling, rich and powerful groups use the exigencies of emergency and collective trauma to push through programs that line their pockets and extend their power at the expense of the less fortunate.[27] To be clear: these interpretations have value. But neither view—infrastructure security as pure theater or infrastructure security as corporate/state power gone rogue—is capacious enough to capture the complex and contradictory changes that have been enacted under the banner of infrastructure security. The cases assembled in this book point to a set of alternate and competing changes: *infrastructure security as public accountability*. Groups that traditionally sit outside of geostrategic security conversations were able to use the threat of terrorism to serve their ends. Greenpeace, the National Association of Letter Carriers, city councilors, and others rarely thought to be key players in the world of national security strategy were able to adopt and deploy the vernacular of the war on terror to carve out a space for expanded public participation in infrastructure. The threat of terrorism offered a potent resource to challenge the infrastructural status quo and, in some instances, enact meaningful change. The politics of security rarely unfold along a straight or predictable path. On the contrary, they include surprising reversals, contradictory changes, and, at times, utterly predictable moves. Ultimately, as the following chapters will make clear, the risk of terrorism circulates and is encoded within infrastructure in surprising ways, both reinforcing and challenging the status quo and alternately comforting and confounding power.

Letters, Power Lines, and Other Dangerous Things develops two key arguments—one a revisionist account of infrastructure history that underscores the political and economic origins of contemporary infrastructure vulnerabilities; the other a rethinking of post-9/11 politics that emphasizes the ways in which fears over terrorism and security were used to justify and enliven (with varying degrees of success) public accountability of infrastructure. These two threads knot together to tell an important story that challenges familiar narratives about the politics of risk and security and forges a revisionist account of the recent political and economic history of infrastructure: it underlines the ways in which fears over terrorism generated new forms of public accountability; it reframes security

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

interventions as attempts to grapple with the legacy of decades of political and economic restructuring in favor of the market; and it offers a pointed reminder that the politics of risk are promiscuous, offering comfort and resources both for the powerful and the marginalized.

The Political Origins of Infrastructure Vulnerability: Regulation and Deregulation Revisited

Our story starts well before the morning of September 11, 2001. To fully grasp the pitched battles soon to be waged over new security practices—the stakes, the key players and coalitions, the surprising reversals, and the stubborn continuities across historical periods—it is important to begin by mapping the larger political and economic history of these networks. This is not just spelunking through history for its own sake and pleasure. Post-9/11 infrastructure changes are in large part attempts to reckon with the legacy and consequences of the political and economic restructuring of infrastructure that occurred during the last three decades of the 20th century. These changes—*deregulation*—set the stage for the post-9/11 transformations that would later unfold in two important ways. First, policies of deregulation worked to create new forms of infrastructure vulnerability. These vulnerabilities would in time become acute sources of political anxiety and, eventually, significant intervention after 9/11. Second, deregulation did more than simply transform the material outlines of how the postal system, freight rail, and electric power operated. The remaking of the political economy of infrastructure was, above all, a political project.[28] It transferred control away from public institutions and their associated norms of accountability in favor of key market participants. This change—the remaking of power within each infrastructure sector—would provide an important context for the later conflicts that would be fought in the early 21st century over how to secure and protect infrastructure.

Deregulation remade the postal, freight rail, and electric power systems. Beginning in the 1970s, the political economy of infrastructure in the U.S. (and across the globe) underwent a seismic change. Infrastructures were deregulated: long-standing public controls that supervised a range of sectors, including communication, transportation, energy, and other infrastructures, were relaxed or rescinded in favor of the market. The wisdom of the market would, the thinking went, substitute for public supervision and stewardship. As Tony Judt observes, the narrow language of economics would now become the principle vocabulary of public policy.[29] The

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

dynamics played out differently in the postal system, freight rail, and electric power, but in each case, deregulation led to a reorganization in both how these infrastructures were managed and in the material contours of these networks. These political and economic changes delivered some real and presumed benefits. In some instances services became cheaper and more efficient, delayed capital improvements were finally realized, and inefficient practices could finally be cut. If nothing else, deregulation pushed infrastructures to become lean and efficient as never before: thousands of miles of freight rail track were abandoned as rail operations were consolidated in the wake of regulatory reform; freed from increasingly arcane methods of budgeting, the postal system moved to replace manual labor with new automated systems for processing the mail; the electric power system responded to deregulation by slashing investment in so-called gold plating (excessively priced equipment and services that were attractive under rate-of-return regulation) and began adopting standard off-the-shelf technologies.

But efficiency came at a price. There were negative costs for workers, particular users, and, ultimately, for infrastructure security. Restructuring pushed infrastructures into increasingly combustible formations. Deregulation led infrastructure owners and providers to adopt what Charles Perrow describes as tight-coupled and complex operational profiles—key changes that placed these systems on vulnerable footing.[30] In each system these changes made new types of large-scale failure possible or more likely. In time, after 9/11, these vulnerabilities would transform into salient political problems. But deregulation did more than interject new types of vulnerabilities into infrastructure systems. It also altered the broad dynamics of power that attended these systems. The rush to embrace the market limited public supervision and control over infrastructure, leaving key market players with significant leverage and the power to define and determine how these services would operate, while workers, environmental groups, local communities, and others with a stake in how infrastructures were organized saw their opportunities to shape these infrastructures comparatively narrowed. The old regulatory model, warts and all, at least held out the possibility of blunting market power with some acknowledgment of larger substantive concerns. Now, market power trumped other concerns.

Understanding this larger historical narrative is important. It demonstrates that the vulnerabilities that became public problems after 9/11 were not ahistorical inevitabilities: they sprang directly and indirectly from a set of concrete political and economic choices. The costs of security,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

then, can be seen as a long-overdue bill—they are in part the unpaid tab of deregulation. Contextualizing contemporary security interventions within this larger historical narrative offers an ironic and wry observation: the ostensible removal of infrastructures from government control in favor of the free hand of the market eventually winds up requiring billions of dollars annually in additional government spending and close, continual government monitoring and controls to make these systems stable. Beneath the continued functioning of liberalized infrastructures sit new risks, massive public expenditures, and increasingly intense governmental efforts to mitigate the newly constructed possibilities of failure.

At the same time, sorting through the twists and turns of deregulation is indispensable for understanding the context and significance of post-9/11 debates over infrastructure security. These debates were never simply about security—they spoke to larger concerns over power and infrastructural control. Drawing the larger historical picture makes this point plain. Fractious debates over who would pay for the added costs of postal security after the 2001 anthrax attacks, fights over the routes that trains carrying toxic material would take, and battles pitting bureaucrats inside the federal government against electric power companies over the proper definitions of critical cyber assets were always about something larger. They were about renegotiating the power to control infrastructure; they were attempts to claw back some measure of public accountability that had been lost through decades of political and economic reform.

Finally, linking these seemingly distinct historical moments—deregulation and later post-9/11 security efforts—highlights the interplay between political economy, the materiality of infrastructure, and risk. As international security scholar Claudia Aradau perceptively notes, critical accounts of infrastructure security often overlook the materiality of infrastructure, reducing these systems to mere "empty discursive receptacles."[31] Indeed, there is a hazard in viewing contemporary debates over infrastructure security too narrowly and treating these systems as neutral or absent objects. This view renders infrastructures as blank canvases upon which contemporary fears about terrorism are projected. Doing so leaches these systems of their history, materiality, and power. It runs the risk of ignoring the agency or power invested in the built world. The materiality of these systems matters. Systems organized in different ways encourage and enable certain types of uses over others—and they encourage and enable different possibilities of failure. Power is inscribed, reflected, and ultimately reproduced within the material organization of infrastructure. Focusing on the connections between deregulation and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

post-9/11 infrastructure security emphasizes how history and power are invested in the material configurations of infrastructure. This is not to say that risks are exclusively material—far from it. The identification, prioritization, and eventual interpretation of particular risks is a deeply social endeavor (as will be discussed in detail below). But, these discursive processes are entangled with the built world. The transformation of infrastructures into dangerous objects—into security problems—is jointly produced through a set of interlocking material and discursive changes.

Ubiquitous Targets: Infrastructure Security after September 11

In the wake of the terrorist attacks of September 11, infrastructure protection and security became a key priority. Now, seen through the exigencies of the expanding global war on terror, infrastructures were quickly transformed in the public imagination into "dangerous things," volatile formations that needed taming and control. Deregulation directly and indirectly went on trial. Decades of political and economic reform created systems prone to fail in spectacular fashion while systematically weakening public controls over these systems. Deregulation's relentless pursuit of efficiency above all else now appeared to be a bad bargain. The political and cultural realignment that occurred after 9/11 made these vulnerabilities legible and salient in a new way. This recasting of infrastructure as dangerous things ultimately led to contradictory changes. New security practices in some instances sealed off infrastructure from public debate and intensified controls targeting workers, users, and suspect network flows. These drastic measures were taken in the name of security. But this is only part of the story. As the second main thread of the book makes clear, novel security practices also led, with varying degrees of success, to new practices of public accountability. A range of groups that traditionally sit outside of discussions of geostrategic security adopted the language of the war on terror to carve out new spaces for public participation and oversight. These practices countered or contested the changes that occurred through decades of political and economic restructuring and opened infrastructures to diverse publics and democratized infrastructure.

The standard account of post-9/11 politics plots a troubling narrative. In this familiar telling, fear, uncertainty, and dread are employed by the state to promote the powerful and justify the diminution of a range of vital civil rights and democratic norms.[32] Mark Danner, writing in the *New York Review of Books* on the occasion of the 10-year anniversary of September 11, offered a sobering appraisal of the politics of the past

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

decade and ventured a worried glance to the future.[33] Danner summarizes the time since September 11, 2001, as

> these years during which, in the name of security, some of our accustomed rights and freedoms are circumscribed or set aside the years during which we live *in a different time*. This different time has now extended ten years—with little sense of an ending.[34]

Danner's appraisal depicts post-9/11 politics as a period of profound and ongoing loss: a period during which cherished values were scarified in the name of security, with little promise of recovery. Stephen Graham's rich tour of what he describes as "the new military urbanism" paints a dismal picture of how these particular dynamics have reworked infrastructures across the globe.[35] Graham recounts how a novel focus on homeland security is leading to the adoption of military technologies and techniques into the conduits of everyday life—infrastructures, once communal and public spaces, are transformed into sites of fine-grained surveillance and control. Graham is not alone in this view; others have also documented in detail how the fear of terrorism props up new forms of surveillance and control that are built into the day-to-day operation of infrastructure.[36] This is the conventional narrative of post-9/11 politics—security fears run amok trample democratic norms and institutions and buttress illiberal constellations. Yet, as the following pages will make clear, the reality of post-9/11 infrastructure and post-9/11 politics is much more complicated and varied. The politics of risk have not only been put in service of the powerful but have worked to democratize and open infrastructure to new voices and new forms of public accountability. This is a counterintuitive finding. The threat of terrorism has been used to *pry open* infrastructure. A cross section of groups, including labor, environmental groups, city and state officials, and others used the vernacular of the war on terror to build out new coalitions and argue for new, enriched forms of public accountability. During the 1970s the language of the market was embraced as perhaps the only legitimate way of discussing or making sense of infrastructure; after 9/11, however, the language of security provided a new vocabulary. The risk of terrorism was not only invoked by the powerful to extend a tight grip over infrastructure. It was also used in nearly the exact opposite fashion: groups that were shoved to the side or fenced out of key decisions thanks to decades of political and economic restructuring now, suddenly, used the threat of terrorism as a way to successfully insert themselves into (or back into) the governance of infrastructure. In some cases these groups were able to enact meaningful change to how infrastructures operate. For example,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the creation of new regulatory powers and standards covering the electric power grid and the transportation of toxic materials has enhanced public accountability in significant and durable ways. It has carved out spaces where interested publics and their representatives can now peer inside the workings of infrastructures and have a meaningful say over how they operate. These are not fleeting or minor changes. Through continual review, enforcement, and rulemaking efforts, regulatory bodies create a record of how infrastructures operate and provide ongoing opportunities for concerned publics to have a say.

The cases assembled in this book challenge familiar readings of post-9/11 politics. The securitization of infrastructure, as the following chapters make clear, was and remains a contradictory process. Reframing infrastructures as security problems leads to both conservative changes that reify and extend existing structures of power and important reversals that open infrastructures in a new and surprising fashion. Accounts that highlight the alarming ways in which counterterrorism and homeland security strategies have bolted military-style strategies onto civilian circuits of exchange are not wrong—but they are incomplete. As the case of the postal system, freight rail network, and electric power grid make clear, the risk of terrorism was, above all, flexible: different groups adopted it for different purposes with different lasting implications. Focusing on the ways in which postal workers, environmental activists, and other groups appropriated the language of the war on terror offers an important observation: the threat of terrorism was used as a tool by those at the margins to split open infrastructure governance and demand that their voices and their concerns be heard. Homeland security as a policy trope and a broader rhetorical framing did not only serve to reinforce the power of those who were already powerful but also served to check and call to account power in important, if overlooked, ways.[37]

Putting the contradictions of contemporary infrastructural changes under a powerful lens helps clarify and extend our knowledge about the political possibilities and limits of risk. Novel risks have a rich—if unpredictable—political power. As Langdon Winner ruefully observed nearly three decades ago, narratives of real and imagined physical harm offer one of the few ways in which technological systems can be meaningfully pulled out of the seemingly neutral world of technology and thrust into the world of politics and critique.[38] But the political possibilities of risk are undetermined. Risk can be used or deployed to serve quite different ends. This is true even of questions of national or geostrategic security, a domain often thought to be rigid and closed. The framing of topics

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

under the rubric of "national security" is typically seen as a way of short-circuiting the normal processes of democratic governance. It is seen as a trump card that allows national security interests to drive out all other voices, ideas, and values.[39] But other dynamics are also possible. As legal and organizational scholar Mariano-Florentino Cuéllar cautions, the politics of security are not monolithic but contradictory and open.[40] The competition to define the outlines of what counts as a security problem is rampant and consequential. As Cuéllar notes, the concept of security is "to some degree malleable," making it difficult to chisel "tidy distinction between geostrategic national security and other types of safety and security."[41] Different topics and areas of concern can be—and often are—framed through the lens of security. In Cuéllar's reading, it is important to avoid "assuming an unusual degree of insularity and consensus in the security space" and instead focus on how particular individuals, coalitions, and interests work to translate security concerns into durable practices.[42] This is vital: focusing on the empirical question of how different groups and individuals work to maneuver the public organizations that actually translate broad, high-level concerns over security into tangible practices is essential. Securitization can spin out in different directions with different implications. Indeed, terrorism has been used by a heterodox collection of actors and coalitions to support a broad array of interests. It has been used to both bolt shut and jolt open infrastructure. These contradictions demonstrate the elasticity of securitization and the fragile possibilities of what sociologist Ulrich Beck refers to as *reflexive modernization*, a process through which novel risks create the scaffolding for new, engaged publics and new forms of political engagement that take aim at the overlooked political choices that sit at the heart of modernity.[43] Tracing the twists and turns of post-9/11 infrastructural upheavals shows that risks can lead to new forms of democratization while offering a bracing reminder that such transformations are by no means inevitable. What ultimately matters are how actors define and fashion particular notions of risk into working coalitions and laws, rules, technologies, and practices. Examining the remaking of infrastructure challenges the ways we often think about post-9/11 politics. It is not a tidy narrative but a story told in fragments: moments of revitalized democratic possibilities and checks on power sit side by side with efforts to dampen public participation and intensify existing hierarchies of power and control.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Theoretical Foundations: Making Sense of Infrastructure

The book borrows liberally from a variety of disciplines and bodies of knowledge, including sociology, political and economic history, science and technology studies, communication studies, and other fields in order to make sense of infrastructure. At its core, however, the investigation is rooted in the insights and possibilities of critical scholarship on infrastructure. Over the past several decades, scholars have created a body of work that takes as its starting point the critical investigation of infrastructure. These efforts, led by Thomas P. Hughes, Susan Leigh Star, Geoffrey Bowker, Paul Edwards, and others, have developed a number of key insights that inform the book.

As a starting point, it is useful to consider the following: What exactly is *infrastructure*? It is a deceptively tricky term to pin down. Geoffrey Bowker and his coauthors give us a useful and elastic initial definition, defining infrastructure "as a broad category referring to pervasive enabling resources in network form."[44] In other words, *infrastructures are systems that support other forms of activity*. This definition is expansive. It includes both physical systems as well as social forms such as the organizations, standards, and protocols that are involved in the provision of these systems. This definition is echoed in current U.S. law and policy. The 2013 Presidential Policy Directive on infrastructure protection offers a similar perspective, stating that "infrastructure provides the essential services that underpin American society."[45] This notion—that infrastructures are systems that sit beneath or "underpin" other forms of activity—is a useful point of departure. It captures the various examples explored in the book, and it also matches how scholars, policy-makers, and others often think about infrastructure.

Moving forward, a few important additional guiding concepts can help flesh out this bare concept. Three core observations drawn from the larger corpus of infrastructure studies help further define how the book approaches and makes sense of infrastructure.

Infrastructures Are Sociotechnical Systems

Infrastructures are bundles of hardware, software, laws, regulations, and ad hoc rules; they join together material systems and the larger world of institutions, organizations, and implicit and explicit assumptions.[46] Treating infrastructures as sociotechnical systems widens the analytic aperture and captures infrastructures as more than just assemblages of technical components. The power grid is often described as the world's largest and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

most complex machine.[47] It is made up of over 180,000 miles of high-voltage transmission lines; 21,437 utility-scale generators that convert coal, petroleum, natural gas, wind, and other sources of energy into electricity; more than 6,900 individual power plants; and myriad substations, transformers, circuit breakers, and switches (to say nothing of the fiber-optic cables, hard drives, monitors, remote terminal units, general and specialized software packages, and other computer and communications equipment essential to keeping the grid up and running).[48] The power grid is, of course, a technical system. *But it is not only* a technical system. It is also a $390.3 billion industry.[49] It is a world of complementary and hostile organizations—private utility companies providing electric power for a price; publicly owned electric cooperatives providing power at cost; state public utility commissions (PUCs) that regulate certain aspects of the electric power grid; federal regulators, which regulate certain *other* aspects of the electric power grid; nonprofit regional transmission organizations (RTOs) and independent system operators (ISOs) that manage and coordinate the grid's transmission network (the key connection that links power generation and local distribution networks); manufacturers that develop and sell all matter of components, from large power transformers that cost more than $7.5 million and weigh over 400 tons to the envelopes used to mail utility bills to customers; and advocacy organizations devoted to any number of issues, including protecting the environment, protecting the fossil fuel industry, protecting consumers, and protecting (after a fashion) the regulators (that would be the National Association of Regulatory Utility Commissioners).[50] The power grid is also a system made up of formal and informal standards and rules. These include state and federal laws, regulations formulated by regulatory bodies, voluntary guidelines developed by industry, and all manner of shorthand used by those working to keep the lights on. Electric power is also a cultural artifact. As David Nye's *Electrifying America: Social Meanings of a New Technology, 1880–1940*, cataloged 30 years ago, it is an artifact freighted with shifting values and meanings.[51] Nye's description of electric power is a fitting epithet for infrastructures as sociotechnical systems: "Someone owns it, some oppose it, many use it, and all interpret it."[52]

Treating infrastructures as *sociotechnical systems* recognizes that technologies are created, adopted, and defined within a broader social context. This is a simple but important point. This approach avoids overly technologically deterministic accounts that view technology as an autonomous actor that bends and shapes society to its will, and it avoids overly socialized accounts that view technology as infinitely malleable putty that

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

is molded to the whims of various social forces and actors. A sociotechnical point of view, as used in this book, focuses on the ongoing interplay between technology and the larger world of organizations, institutions, and culture. It is in this intersection that infrastructures are created, sustained, and transformed. Technologies rarely appear fully formed. What in retrospect looks like a clear or linear trajectory from invention to later adoption and institutionalization is, in fact, filled with the messy stuff of history—competing technologies, unsettled uses, confused and unruly users, rival standards, and long-forgotten alternative ways of organizing and deploying a technology. Technologies offer a range of different possible uses or configurations, a set of different possible branching pathways, but it is left to organizations, institutions, and cultural understandings to clear, mark, and enforce these paths—winnowing down available options into a defined set of organizational forms, uses, and meanings. To make sense of how the post office, freight rail network, or electric power system were created, remade during the waves of deregulation that began in the 1970s, and then again remade after 9/11 requires mapping how infrastructures are at once social and technological formulations. The book takes as its starting point that infrastructures are more than wires, steel, and chips. They are a complex set of interacting technologies, organizations, institutions, and cultural assumptions. It is in this collision that infrastructures can be usefully analyzed and understood.

Infrastructures Are Relational

Infrastructures lash and bind infrastructure workers, owners, regulators, different types of users, and different sorts of uses into a particular set of relationships.[53] Power is central to infrastructure. No two groups are likely to relate to an infrastructure in the same way. Infrastructures create publics: groups defined in part by their connection to the larger systems. These different infrastructural publics see and relate to infrastructure in different ways.[54] The postal system offers a useful example. For letter carriers, the postal system is a job. It is a source of joy, frustration, sociability, economic support, and other workplace mundanities. For a rural community underserved by for-profit delivery services, it is a lifeline. It delivers medicine and other vital goods at comparably low costs. But for the staff at the Postal Regulatory Commission (previously known as the Postal Rate Commission), the postal system exists as a set of data to be scrutinized. Here, the postal system appears most readily as a collection of statistics on mail volume, processing costs, and other information deemed relevant for setting and adjusting rates. Direct-marketing

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

agencies peddling circulars, political advertisements during the run-up to an election, and other postal ephemera see the postal system as an important way of reaching and selling access to targeted audiences. For some postal customers, the postal system is little more than a nuisance—a spigot distributing an unyielding supply of junk mail. Writing in 1970, Chief Justice Burger summarized this view well, noting that "whether measured by pieces or pounds, Everyman's mail today is made up overwhelmingly of material he did not seek from persons he does not know. And, all too often, it is matter he finds offensive."[55] To others, though, the postal infrastructure is a (still) cherished source of connection—it is the seemingly magical system that brings a child a birthday card from an out-of-town grandparent.

Different groups relate to infrastructure in different ways. Infrastructures are, as noted above, platforms for other forms of activity. But they are not neutral platforms. They organize a mix of users, uses, owners, workers, and regulators in a particular set of relationships. Digging even an inch under the surface of infrastructure reveals power and hierarchy. Certain users get favorable terms, while others face subtle and overt barriers to access and additional costs. Various types or work are rewarded, while other forms are viewed as disposable or unacknowledged. Particular types of uses are valued and promoted at the expense of others. Workers, owners, regulators, and customers rarely agree on the best or most equitable terms of infrastructure operation. Each makes different and at times competing claims regarding how the system should run and what its purpose or importance is. The book places power and control at the center of its analysis. In examining the twists and turns of these various systems, it sees infrastructures as sites of ongoing conflict. As Finn Brunton's history of unwanted electronic mail—spam—details, technologies are spaces of significant *drama*.[56] Brunton, following Bryan Pfaffenberger, identifies technologies as stages for social and political arguments precisely because they organize and distribute power.[57] Different interests spar and seek to renegotiate the organization and arrangement of these various infrastructural relationships.

This book is particularly interested in the interplay between organized interests (corporations, regulatory bodies, advocacy groups, and others), larger cultural narratives, and infrastructural control. The transformation of infrastructure into dangerous things after the terrorist attacks of 9/11 was in part a cultural upheaval (as was, to a degree, the reimagining of infrastructure during the last quarter of the 20th century as free market avatars). What is most fascinating, however, is how

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

organized interests worked to leverage this newly salient cultural meaning of infrastructure to rework the laws, regulations, and technologies that make up these important sociotechnical systems.[58] Larger cultural narratives and logics are powerful, but they need allies—identifiable actors—to forward these ideas and shape them into concrete programs. The book focuses on how competing groups advance different claims to infrastructure and seek to alter the ways they stitch together heterodox groups and uses into a larger fabric. Conflict and power are central points of focus throughout the text.

Infrastructures Are Historical

Infrastructures are shaped by decisions that occurred decades, if not centuries, earlier at constitutive moments. In other words, infrastructures are path dependent. Once a particular way of organizing an infrastructure is in place, it becomes difficult to shift gears and enact meaningful, large-scale change. Richard John and Paul Starr identify these dynamics in U.S. communications history. They observed that once in place, particular models of governing the postal system, telegraph, and telephone were difficult—though not necessarily impossible—to change.[59] Thomas P. Hughes and Richard Hirsh identify similar path-dependent processes at work in the electrical industry.[60]

The overlapping legal, regulatory, and platform aspects of infrastructure work in favor of path dependency. Each of these features contribute to the "stickiness" of infrastructure. First, infrastructures are, in part, enshrined in law. Statutes touch on various aspects of infrastructure operation. Laws relating to infrastructure, like all laws, are difficult to change. As Paul Pierson argues, law itself is path dependent: majoritarian politics creates collective action challenges that ultimately favor keeping existing laws and legal regimes in place.[61] It is easier to live with the current law than to collect the votes needed to enact something—anything—new. Second, regulations also contribute to infrastructure inertia. Regulations are seemingly easier to alter than laws. Regulations formulated by regulatory bodies or rules enacted by administrative agencies do not always face the same degree of collective action challenges that confront the creation or modification of laws. Changing specific regulations does not necessarily require congressional authorization. Depending on the particular regulatory body, the agreement of a majority of regulatory commissioners is often all that is needed, a lower bar than what is required to enact legislation. But regulations also have inertia. Law and regulations help to organize infrastructure in certain ways. They favor some groups over

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

others. Once particular regulations are in place, the constituencies that benefit from them fight to keep them in place. Interest groups cajole, pressure, and otherwise work to ensure that regulators maintain the status quo, helping to buttress the collective action challenges that favor the status quo. Third, the nature of infrastructures as platforms is a key contributor to path dependence. Generally, infrastructures underlie vast industries. These industries may, from time to time, push back and challenge existing laws and regulations, but there is a bias in favor of the status quo. This is due both to the fact that regulatory stability is preferred over unpredictable and sharp changes and, most importantly, because the legal and regulatory foundations of infrastructures are reproduced in the very structure of the industries that sit atop infrastructures. In other words, particular legal and regulatory outlines become chiseled within the larger industrial outlines. Take, for example, the freight rail industry during the late 1800s and early 1900s. After cycles of boom and bust, laws and regulations devised by the Interstate Commerce Commission (ICC) moved to stabilize a particular version of the rail industry—they protected large national and regional cartels (over diverse ownership); they favored shipments of raw materials over finished goods; and they favored protecting existing track and lines over consolidation and abandonment. Once these legal and regulatory protections were in place, organized interests, the railroads, key shippers, and others fought to keep them in place. The laws and regulations made these interests more powerful, which in turn intensified their advocacy for the status quo and made change more difficult. The particularities of law and regulation became increasingly rigid as they became ground into a set of ever more powerful complementary organizations. These overlapping legal, regulatory, and platform aspects of infrastructure contribute to path dependence. That is not to say, as we will see, that significant structural changes are impossible. It just means that such changes are difficult and rare.

The book focuses on three key constitutive moments: (1) the initial formation or consolidation of infrastructure, (2) the deregulation of infrastructure during the 1970s–1990s, and (3) the reordering of infrastructure after 9/11. Each of these three moments are important because they shaped these sociotechnical systems in important and transformative ways, creating pathways that would endure for significant periods or, in the case of the post-9/11 changes, appeared as though they would be difficult to change. Focusing on these moments underscores a key feature of infrastructures: they are historical artifacts. They are a palimpsest of long-ago decisions. Choices made for good, obscure, or poor reasons over time

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

become engrained in the workings of infrastructures. Looking closely at these various key periods highlights both the durability of infrastructural orders and the ways in which they can, under certain conditions, become reversed or altered.

These three features of infrastructures—*infrastructures as sociotechnical systems*; *infrastructures as relational*; *infrastructures as historical*—guide the investigation that follows.

Theoretical Foundations: Making Sense of Risk

The concept of risk is also central to the book. How are particular objects made dangerous? How and why are certain hazards prioritized as political problems, while others are dismissed? The book takes risk to be a socially constructed material and discursive artifact. As developed here, this view of risk focuses on power—how power can create risk and how risk can, at times, serve to provide the political capital needed to confront entrenched power. This approach breaks with classic accounts of risk in economics and hews more closely to the sociological treatments of risk found in Charles Perrow's theoretical work on *normal accidents* and in Ulrich Beck's concept of *risk society*.[62] Perrow and Beck make a somewhat unusual pairing: Perrow's work is empirically detailed and focuses on the concrete ways in which organizations create new types of risk; Beck is prone to sweeping theorizing and is interested in how certain types of risk create new political possibilities. Taken together, however, they allow us to look at the consequences of deregulation and explore how risk circulates as a cultural and political resource.

In his foundational economic text, *Risk, Uncertainty, and Profit*, Frank Knight offers a straightforward definition of risk: risk is a measurable type of uncertainty.[63] It is a future possibility that can be calculated through the accumulation of historical data or other quantitative means. It is the calculation of the likelihood (and severity) of a given future event.[64] Against this notion of risk as something that can be calculated, Knight presents *uncertainty*: possibilities that resist quantification.[65] In lay conversation, Knight points out, these two phenomena—risk, which is measurable, and uncertainty, which is not—are often incorrectly blurred.[66] This notion of risk, as Andrew Lakoff notes in his overview of the concept, underlies techniques of technical risk assessment.[67] These techniques have been deployed by governments to determine and improve the welfare of populations against disease, accidents, and all manner of misfortune.[68] This approach to risk, as Lakoff reviews, has been criticized on

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

a number of fronts. Most significantly, science and technology scholars have questioned the ways in which technical risk assessment masks hidden assumptions and values and marginalizes lay knowledge.[69] That is, it obscures or ignores power.

The work of Charles Perrow offers a useful way of examining risk from a different angle. Perrow is most interested in the intersection of organizations, power, and risk. Perrow coined the term *normal accidents* to describe failures rooted not in operator error or pure chance but rather in systemic properties.[70] In this view, systems that are tightly coupled and complex create the conditions for normal accidents. These accidents are "normal" not in the sense of frequently occurring but rather because they are the expected results of particular forms of systemic organization.[71] This is far afield from Knight and classic risk assessment. It says little about frequency or likelihood and concentrates instead on the possibilities of failure. It focuses on how systems become vulnerable or prone to failure, rather than the creation of tables recording historical incidents. Normal accident theory offers a vocabulary to qualitatively examine technical systems and organizations. In particular, it provides a way of thinking about and assessing the materiality of risk while still acknowledging that these risks are, at bottom, socially constructed; it offers a framework to examine how the various ways of arranging the technical and organizational outlines of systems have different possibilities of failure. In the pages that follow, this framework helps to make sense of and evaluate the material changes that occurred within the post office, rail system, and electric power grid. We can plot these systems as they move from loose to tightly coupled and from linear to complex. As they move across these planes, new forms of failure—including accidents, complications from natural disasters, and even terrorism—are now made possible or expanded. The adoption of centralized processing plants, just-in-time delivery models, complex software, and other changes can be scrutinized through this lens. But Perrow offers something larger than just a framework for assessing the material foundations of risk: he offers a reminder to connect the organization of these technical systems to larger currents of power. His work makes this point plain: material systems are socially constructed—they reflect and are defined by the organizations and larger political and economic institutions that surround them.[72] Technologies cannot be wrenched from their larger organizational and institutional context. To understand why or how a particular system becomes vulnerable in new ways requires working through the connections between organizations, institutions, and power. This book works in this spirit, using

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

normal accident theory to evaluate or make sense of the ways in which deregulation reordered infrastructure.

Normal accident theory is helpful in evaluating how deregulation transformed the post office, freight rail system, and electric power grid into vulnerable configurations. But it says little about how these systems and their attendant risks became public problems or how these risks were ultimately translated into particular security practices. Here, the work of Ulrich Beck is indispensable. While Perrow focuses on the social construction of material risks, Beck offers conceptual tools to explore how risk circulates as a cultural artifact and political resource. Beck argues that contemporary life is in the process of becoming a risk society.[73] Modernity is creating new forms of risk that cannot be calculated and managed through the usual tools of government and science.[74] These new forms of harm are incalculable, potentially catastrophic, and, importantly, generated by the very processes of modernization. Beck argues that these sorts of risk are politically explosive.[75] They can serve as the foundation for new political coalitions and new ways of organizing. They can lead to the democratization of areas of social life—such as the economy, fields of science and technology, and politics—that are shut. But these are only possibilities. Beck is quick to point out that risk on its own cannot compel anything—it requires groups to mobilize and work to translate the political possibilities of risk into durable and specific programs.

Beck's account is useful in highlighting how infrastructure risk circulates as a volatile and promiscuous political resource. His work can help to better understand how the post office, freight rail network, and electric power grid became salient problems. Now we see the overlapping cultural, organizational, and institutional processes that worked to highlight these particular risks (over myriad others) and transform these systems into objects of concern and, ultimately, action. Perrow can help us map how these systems became prone to new forms of failure, but Beck assists in sketching how these possibilities became salient and politically transformative. Taken together, Perrow and Beck offer useful points of departure for thinking about the contemporary reordering of infrastructure as dangerous things.

The Structure of the Book

The main body of the text is divided into two broad thematic sections. Part I, "The Political Origins of Infrastructure Vulnerability," explores the social and material impacts of the regulation and eventual deregulation of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the postal system, freight rail network, and electric power system. Part II, "Ubiquitous Targets: Infrastructure Security after September 11," examines the post-9/11 remaking of these infrastructures. It considers how new anxieties over terrorism and infrastructure subversion worked to transform each of these sociotechnical systems. Here, the book documents the *bureaucratization of risk*: how fears over terrorism were translated and encoded into new laws, regulations, technologies, and practices. The conclusion and coda examine the importance, limitations, and contradictions uncovered within these three specific case studies.

Chapter 1, "Stumbling toward Resilience: The Overlooked Virtues of Regulation," examines the historical foundations and practice of regulation within the postal system, electric power grid, and freight rail network. Regulation appeared in a slightly different guise across each system. In each case, law and policy shaped the social and material outlines of these systems in specific ways. Regulation offered a degree of public accountability over infrastructure: it organized the warring set of competing interests—different infrastructure publics—that surround these networks and carved out a space for public participation in infrastructure governance. Regulation also directly and indirectly shaped core decisions concerning the material organization of these systems—the broader structure of regulation found expression in these systems' smallest details. Chapter 1 uncovers the hidden and not-so-hidden benefits tucked within the old regulatory models. In addition to stabilizing these systems and providing the public with venues to air their concerns, regulation, in its various forms, worked to promote resilient systems. Regulation supported systems that were fault-tolerant: failures (from accidents, natural disasters, or intentional disruption) were local in scope and limited in size. Chapter 1 introduces normal accident theory, a key touchstone for the rest of the text, in more depth.

Chapter 2, "The Political Origins of Infrastructure Vulnerability: The Hidden Vices of Deregulation," turns to examine how deregulation remade the postal system, freight rail network, and electric power grid. Political restructuring led to a host of social and material changes. Deregulation was incomplete: although state supervision was not entirely swept away, on balance, reform drastically renegotiated the balance of power between the state and various infrastructure publics. The chapter traces how restructuring gave key market players enormous new power to define how these infrastructures operated while leaving other groups on the side. Deregulation also led to the gutting of support for resilience. It promised to sweep away the inefficiencies of the old regulatory model and sought to create new lean infrastructures trimmed of the "fat" that

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

had accumulated under state stewardship. But these changes came at a price. Political restructuring pushed these systems into increasingly combustible formations. Chapter 2 reveals the hidden and overlooked costs of deregulation. The drive to improve efficiency created systems that were ripe for large-scale failure and increasingly sealed off from substantive public control. It was precisely these new possibilities of failure that would reappear after 9/11 as pressing and difficult public problems, and it was this power dynamic that would be tested and, in some cases, upended through new forms of infrastructure security.

Chapter 3, "Imagination Unbound: Risk, Politics, and Post-9/11 Anxiety," considers the interlaced post-9/11 cultural, institutional, and organizational changes that worked to transform infrastructure vulnerabilities into public problems. The material changes ushered in through deregulation created new possibilities of failure, but these material reorderings were only legible as security problems thanks to the changes enacted after 9/11. Now, infrastructures were viewed through the lens of the war on terror. The development of homeland security policy helped legitimize the notion that infrastructure can and should be thought of as dangerous objects in need of protection—a key cultural shift or reshuffling. Organizational and institutional changes supported this conception of infrastructure and set the stage for the fractious battles over how, exactly, new forms of security would be put into place. This chapter looks closely at the work of Ulrich Beck and spotlights the important social changes that underlie the transformation of infrastructure into dangerous things.

Chapter 4, "Infected Mail: Labor, Commerce, and the 2001 Anthrax Attacks," begins a series of three chapters that focus on how new forms of security were invented and deployed within each infrastructure sector. This chapter focuses on postal security. It critically investigates the new security practices that the United States Postal Service (USPS) put into place after the 2001 anthrax attacks. Eventually, USPS adopted two new systems: the Biohazard Detection System (BDS) and Intelligent Mail. Postal management, labor, large commercial mailers, defense contractors, and local communities fought bitterly over the terms of postal security. Labor used the threat of terrorism to open up postal governance and secure access to high-level technical advisory boards. These gains, however, were short-lived and modest. Ultimately, the interests of large commercial mailers were encoded within the architecture and operation of both the BDS and Intelligent Mail. Chapter 4 examines the minutiae of these surveillance systems and uncovers the retrenchment of powerful interests at the expense of postal labor and the larger public.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Chapter 5, "Green Security: The Environmental Movement, the Transportation of Hazardous Materials, and the War on Terror," examines the creation of new security regulations governing the rail shipments of hazardous materials. Chapter 5 charts how activists—for example, Greenpeace, Friends of the Earth, the Sierra Club—local public officials, and select members of Congress adopted the vernacular of the war on terror in order to secure tougher controls over shipments of hazardous materials. The threat of terrorism provided a new rallying point for environmental activists and a new means of building an effective policy coalition. It allowed previously marginalized actors to assert their voices, to overcome stiff opposition from rail and chemical lobbies, and, ultimately, to substantively change transportation law and policy. While chapter 4 offers a window into how the political possibilities of risk can be put into the service of the powerful, this chapter highlights how marginalized groups can leverage the risk of terrorism to check the power of market players and create new forms of accountability over infrastructure.

Chapter 6, "Regulating Cybersecurity: The Unexpected Remaking of Electric Power," sketches the development and implementation of new cybersecurity regulations for the electric power grid. These regulations grew from what initially appeared to be industry-friendly legislation and thin administrative powers into a robust system of public accountability. Here, as in chapter 5, risk provides a key political resource that was put into service to address the material vulnerabilities and social transformations of deregulation in a meaningful way. The expansion of regulatory authority effectively democratized infrastructure governance. Under the newly adopted regulatory regime, the public, regulators, and concerned parties can now participate in the draft, review, and implementation of mandatory standards. Rather than having decisions over the grid decided by industry through closed-door negotiations, the process is transparent and accessible.

The book draws to a close with a short conclusion and coda. The conclusion, "The Politics of Critical Infrastructure Protection," steps back to review the three cases. After 9/11 the political project of deregulation was put on trial. The triumphant boosterism of free markets, corporate power, and a deferential state began to sound tin. Policy-makers wrestled with the consequences of deregulation and tried to patch new forms of security onto these vast and complicated sociotechnical systems. The conclusion takes stock of these efforts and finds the complicated legacy of 9/11 recorded in the intricate workings of infrastructure.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The coda, "Infrastructure as Target," expands the book's frame to look beyond infrastructure protection and security efforts and toward the development of offensive capabilities targeting infrastructure. While U.S. policy-makers and other interested parties worked to design new forms of infrastructure security, the government also worked to create new, secretive, state-sponsored tools of espionage and sabotage that threatened to undermine these gains. New intelligence-gathering techniques and hacking tools threaten infrastructure security both at home and abroad. The coda examines the U.S. defense and intelligence communities' efforts to weaken encryption standards and create stockpiles of previously unknown and undisclosed software vulnerabilities—what are known as *zero-days*. The text documents how efforts to target the infrastructure of our adversaries (and even, sometimes, our allies) can undermine the security of domestic networks. While the U.S. is spending tens of billions of dollars annually on critical infrastructure protection, deep in the "black budget" are efforts designed to preserve flaws, prevent the adoption of robust protections, and, generally, promote insecure systems. The coda considers the tension between homeland security and the creation of tools that target infrastructure for offensive purposes. The book draws to a close with a mordant question: Is the best defense, perhaps, a weak offense?

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

I

The Political Origins of Infrastructure Vulnerability

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

1

Stumbling toward Resilience: The Overlooked Virtues of Regulation

Long Island Lighting system operator: "Can anyone tell me anymore [*sic*] what happened to Con Ed?"

New York Power Pool senior dispatcher: "It looks like he is all by himself right now; looks like he's separated from the system."

Long Island Lighting system operator: "From everybody?"

New York Power Pool senior dispatcher: "Yep …"

—Telephone call between New York Power Pool senior dispatcher and Long Island Lighting Co. system operator, July 13, 1977[1]

At 8:37 p.m. on July 13, 1977, lightning struck two extra-high-voltage transmission lines in Westchester County, just north of New York City.[2] The lines were part of Consolidated Edison's (Con Ed) electric power system, which supplied electricity to most of New York City and parts of Westchester County. At 8:56 p.m. lightning struck two additional Con Ed high-voltage lines.[3] The system was significantly stressed. At 9:36 p.m. the entire Con Ed system failed. Over 8 million people in New York City and Westchester were without power.[4] The blackout lasted over 24 hours. In the city, reports of looting and arson quickly followed—1,037 fires, six times more than normal, were reported for the evening, and over 3,000 people were arrested.[5] This disorder following the loss of power was interpreted by the press as symptomatic of larger economic and social tensions endemic to the city.[6] *Time* magazine's grim report on the blackout was titled "Night of Terror"—quoting a description offered by New York mayor Abraham Beame.[7] A spokesman for Con Ed described the failure as "an Act of God."[8]

Yet just a few miles away, in nearby Rockaway Beach, the lights stayed on. Playland, an amusement park, was open for business.[9] Patrons filled

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the park, and go-carts and roller-coasters operated without interruption.[10] The next morning the *New York Times* observed the ironic juxtaposition between Rockaway and the rest of New York City in a story headlined, "Still Fun City in Rockaway Peninsula."[11] While the majority of New Yorkers were without power, for the 98,000 people in Rockaway, it was a regular summer night. At the Paddy Wagon Bar, reporter Ari Goldman wrote, "The juke box was blaring and several customers played the electric pinball machine."[12] The blackout was isolated to Con Ed's system. Rockaway and Long Island, both served by Long Island Lighting Co., were spared, as were the surrounding Rockland and Orange Counties in New Jersey, which also fell outside of Con Ed's system.[13] The outage could have been worse. For decades a mix of federal and state regulations had worked to create a network of loosely joined electric power systems. Regulation had prevented the consolidation of local networks into larger regional configurations. The blackout was devastating for New York City, but it was a local failure. The surrounding systems—Orange & Rockland Utilities, Central Hudson Gas & Electric Corp., Long Island Lighting Co., Niagara Mohawk Power Corp., Public Service Electric & Gas Co., Connecticut Light & Power Co., and others—were able to disconnect from Con Ed and continue providing power to their customers with minimal interruption.[14] The blackout did not spill over into other adjacent electric power systems. In this way the 1977 blackout was typical of power outages of the era: power outages that crossed system boundaries, such as the blackout of 1965, were exceedingly rare. Federal and state regulations, though designed for other purposes, helped create an electric power system that was resilient. Regulatory geography proved to be incredibly consequential: while Con Ed's system plunged into darkness, the larger regional network was able to thrive. Playland stayed open.

* * * *

This chapter revisits the regulatory history of the postal system, freight rail network, and electric power system. From the late 18th century until the last quarter of the 20th century, U.S. law and policy oversaw and controlled infrastructure operation through a variety of regulatory means, including regulation by federal bodies, oversight by state public utility boards and commissions, and, in some cases, limited federal ownership and operation. In each case, supervision hinged on the control of price (how much infrastructure providers could charge for different forms of service) and entry (who could legally offer services). *Price-and-entry* regulation offered a host of obvious benefits: it protected consumers from

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

discriminatory practices; it ensured that services were built out and extended across territories and populations; it blunted ruinous competition that threatened to capsize companies seeking to build and operate infrastructure enterprises; it provided operators with stable returns that could be reinvested into service improvements; and it limited the ability of well-positioned incumbents to use their influence to manipulate and dominate other industries. The creation of a vast regulatory machine served (with varying degrees of success) as a counterweight to the power of key infrastructure operators and powerful customers. It worked to enact a quid pro quo between various infrastructure publics—different groups bound together through these sociotechnical systems. Regulation provided an important means of making infrastructure publicly accountable: it served to ensure that substantive political values, such as nondiscrimination and access, were built into infrastructure operation; it offered a venue for diverse interests to air their concerns; and it provided at least the possibility of pushing back against dominant market players. But regulation provided another often-overlooked benefit: *resilience*. Regulation worked to support networks that were resilient to large-scale failures. Regulation militated not only against the deleterious effects of concentrations of economic and political power but also against dangerous concentrations within the architecture of infrastructure services and systems. Price-and-entry controls, both directly and indirectly, promoted distributed control within these systems. They created systems with a degree of flexibility; although these networks had internal connections, islands of autonomy were built into the systems. Loosely coupled independent fiefdoms and vertices of control were nested within the postal system, the freight rail network, and the electric power grid. At the same time, regulation supported the adoption of linear—rather than complex—operational profiles. These qualities—loose coupling and linearity—provided a hedge against large-scale and systemic failures. Later, during the political upheavals of deregulation that began in earnest in 1970, these very qualities came under attack as evidence of the failings of regulation. Ironically, these perceived failures of regulation provided, to differing degrees, a margin of security and safety that post-9/11 infrastructure interventions would seek to recapture.

To understand how and why infrastructures later turned toward increasingly vulnerable configurations, it is crucial to first examine regulation's role in directly and indirectly shaping these systems (and the role these systems played in shaping regulation). Infrastructures are embedded within a thicket of regulatory practices; these sociotechnical systems join

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

technical components with particular organizational and institutional arraignments.[15] It is only through a historically informed understanding of the particularities of regulation that we can make sense of why infrastructures appear as they do. Regulation played a central role in molding the postal system, freight rail network, and electric power system: it compelled and favored certain configurations, sets of users, and uses while forbidding or discouraging others. Only after foregrounding regulation can we understand why, for example, the Post Office Department continued to rely on manual letter sorting long into the 1960s, after more efficient mechanized and automated equipment became available, or why for decades the cost of shipping a ton of grain via rail was far less expensive than shipping a ton of industrial chemicals, or why electric power systems were organized into a set of local and regional systems, rather than larger configurations. Without examining the ways in which infrastructures are lodged within regulatory processes, these and many other "quirks" of infrastructure design and operation remain difficult to parse.

Regulation appeared in a slightly different guise across each system. In each case, regulation emerged less from grand design than through a mixture of happenstance and conflict between various infrastructure publics. Once in place these regulatory schemes became rigid: they molded how these infrastructures would develop. In postal communication, the U.S. government operated the main elements of the postal network directly through the Post Office Department and controlled price and entry through a limited legal monopoly and congressional stewardship. In rail, an independent federal regulatory commission—the Interstate Commerce Commission (ICC)—set rates, adjudicated disputes between shippers, railroads, and other infrastructure publics, and promoted a large set of rules regarding entry and exit. In electric power, a mix of federal and state laws created and protected a system of vertically integrated local monopolies that were loosely joined at the edges; state utility commissions oversaw the basic terms upon which utilities operated, and federal law limited the growth of systems into unwieldy configurations. In each case, regulatory interventions shaped core decisions concerning how to organize these large systems. Buried within the minutiae of regulatory policy and practice were greatly consequential decisions. The accumulation of numerous "small" choices—deciding between different ways of assessing costs, divvying up congressional committee assignments, devising formulas for how to factor capital and research and development expenses into standard rate calculations, figuring out how traffic patterns should or should not change after the merger of a small regional railroad and a larger line,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and many others—reverberated loudly. Over time, the particularities of regulation became encoded within these infrastructures, drilled into the material inner workings of these systems.

Importantly, as we will see, regulation pushed the development of each system in directions at odds with a narrow conceptualization of economic efficiency and held out the possibility of public accountability while, at the same time, incidentally or accidentally supporting resilient networks. To be clear: these resilient features were not understood or recognized at the time. It was only in retrospect, after deregulation had undermined these aspects of these networks and as specific post-9/11 cultural, institutional, and organizational changes worked to reframe infrastructures as security problems and sites of anxiety, that these "vices" of the old regulatory model would appear as virtues. To understand how the postal system, freight rail network, and electric power grid were made dangerous, we must first start with a wonkish deep dive into regulatory history. Revisiting regulatory history through the lens of the present starts our genealogy of infrastructure insecurity. It offers a wry observation: the old model of regulation, much decried and rarely celebrated, worked to build systems that were resilient.

Normal Accidents: Complex Networks, Tight Coupling, and Failure

Before discussing how regulation supported the construction and maintenance of infrastructure systems that were, in key respects, impervious to large-scale failure, it is first necessary to provide a conceptual framework for assessing the characteristics that define the resiliency and vulnerability of large technical systems. Resilience has become something of a buzzword in policy circles, but the concept remains often maddeningly vague: What exactly is a resilient system?

Charles Perrow's work on normal accidents offers a useful conceptual framework.[16] Rather than seeing large-scale failures as simply the product of operator error or caprice, normal accident theory redirects attention toward the different ways that system architecture and organizational imperatives can create the conditions for large-scale failure.[17] Perrow labels these types of failures *normal accidents* because the roots of failure are embedded within the structure of the larger system itself. There is a simple yet indispensable insight at the heart of normal accident theory: differently arranged systems are prone to fail in different ways. Although the notion of normal accidents was initially derived from an examination of industrial accidents, as Perrow notes, the same qualities

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

that render systems prone to accidents also increase the possibility of failures from natural disasters and malicious, intentional disruption from acts of sabotage or terrorism.[18]

Perrow's framework revolves around two central concepts: complexity and coupling.[19] Differing degrees of complexity and coupling within a system determine the difference between resilient systems that can tolerate disruptions and systems prone to large-scale failures. Complex, as opposed to linear, systems are defined by reliance on common-mode components—technologies that link multiple elements within a system—or by the grouping in close proximity of different unrelated systems.[20] Common mode technologies and proximity creates unexpected interactions—complexity—that can lead to systemic failures. The failure of common-mode equipment, for example, does not lead to a simple, localized serial failure in the next step of a sequential process; it can spark unpredictable failures across the system. In linear systems, components are organized in sequence. Each step leads to the next; and each technology is dedicated to a specific task. A failure of any single part of the system breaks the chain (think here of a simple assembly-line system) and causes a minor disruption until the failing component can be fixed or replaced. Take, for example, a classic episode of *I Love Lucy*, "Job Switching." In this episode Lucy and Ethel work on a conveyor belt at a candy factory wrapping chocolates. As the candies roll by, the hapless workers are increasingly unable to keep up—stuffing chocolates into their mouths, shirts, and hats. This is a linear failure. The screwup is a problem, but a relatively manageable and small one. It has a straightforward and predictable impact—the assembly line backs up, and, presumably, the candies cannot be packaged and shipped. Fixing this sort of problem is also, more or less, simple: slow down the belt or add more workers on the line.

In complex systems, however, failures are more difficult to manage. They have unpredictable effects.[21] The failure of a common-mode connection linking different portions of a process, such as an interconnected computer system controlling billing, production, and distribution for a manufacturer, not only causes a delay in one small isolated or containable area but spins outward in unexpected ways, affecting various areas of operation.[22] Let's now imagine an *I Love Lucy* update loosely based on the Heartbleed vulnerability in OpenSSL (an open-source software library).[23] Lucy and Ethel aren't working in the candy factory; they are software developers writing code for an open-source software library. This library contains code that is freely used and deployed in all sorts of applications to provide secure communication. Lucy suggests a particular

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

change to the library and Ethel, a core developer on the project, approves it. But Lucy's work contained a bug that neither she nor Ethel noticed. Later, clever researchers discover the mistake. It turns out that *any* application that uses Lucy's code accidentally leaks sensitive password data. But it is too late. The bug has already been reproduced in all sorts of software applications that have nothing in common (a university's student enrollment-tracking application; a bank's online portal; a fitness app on your phone) besides the fact that each has baked Lucy and Ethel's buggy code into its current build. These applications are all now vulnerable. Unwinding this problem will not be simple. This is a complex system. First, teams across any number of organizations are going to have to quickly (and nervously) determine whether they even used this buggy code in the first place. Did they use Lucy and Ethel's code in their software? If they did, they will then have to work to develop or adopt (if they are available) mitigations and updates that fix this problem (while testing to make sure that this update does not cause additional unforeseen problems or issues). In both cases, Lucy and Ethel made simple mistakes. But in the linear system—the candy factory—the impact was obvious, straightforward, and predictable. The second example is different. The technology is complex—it is deployed and used in all sorts of software applications. In this case, Lucy and Ethel's mistake has nonlinear effects. A mistake made on a laptop in Lucy's apartment has impacts that she could not imagine—that's the difference between a linear and a complex system. Linear systems fail in unsurprising (though maddening and frustrating) ways. The impacts and fixes are clear. Complex system failures are different. The failures are difficult to anticipate, and they have far-reaching effects that are hard to foresee—and hard to fix.

It is not just a reliance on common-mode equipment that can drive complexity. Complexity can also grow out of proximity. Putting two or more different systems or subsystems near each other can lead to unexpected interactions. Here, these interactions come not from common-mode equipment or technologies but from these unrelated systems' geographic closeness. A failure within one system or subsystem jeopardizes another system that is formally distinct but nearby; a failure in system X causes a disruption in system Y simply by virtue of colocation.[24] Let's consider a hypothetical and particularly ill-advised bit of public planning. Imagine placing a hospital and a local elementary school on the same street. The hospital has a large parking lot and space for ambulances to quickly pull up and unload patients to the emergency room. So far, so good. The hospital is well designed to handle both regular visitors (the parking lot has

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

ample spaces) and emergency patients. Next door is an elementary school. It has a small parking lot, with just enough spaces for each teacher and staff members to park. Out front, there are "no parking" signs in front of the school. This keeps the area open for pick-up and drop-off. On school mornings, parents and school buses pull up out front and unload excited elementary school children. This system, like that of the hospital, seems well designed. But, when these two systems—the school and hospital—are put next to one another new failures become normal. Neither system was necessarily designed with the other in mind. On busy mornings, the lineup of buses and parents eager to deposit their kids at school will clog the street, making it difficult for ambulances to reach the hospital in a timely manner. During special occasions—a school play, a musical performance, parent-teacher conferences—parents will park in the hospital lot and take spaces away from hospital patients and their families. Problems will flow in the other direction too. Ambulances arriving with sirens blaring will constantly disrupt and annoy students and teachers alike. As this very simple example shows, colocation can lead to unexpected and nonlinear interactions. Proximity, as this example highlights, can lead to unexpected interactions across systems, with large consequences. Proximity between different systems increases complexity in that it injects another variable, the action of the adjacent system, for which the neighboring system is not designed to cope.

Perrow's second key concept, coupling, refers to the degree of slack in a system. Perrow offers a distinction between loose and tightly coupled systems.[25] Tightly coupled systems are characterized by time-dependent processes that cannot be slowed down, invariant operation, and little independence of components (Lucy's conveyer belt is linear, but it is tightly coupled).[26] The strict conditions of time dependence eliminate any moment for the system to regroup, while invariant operations do not easily admit substitutions or ad hoc changes. But most significantly, tightly coupled systems favor centralized and rigid control: clear rules must be followed—there is only *one* way that things can be done; there is no room for improvisation or ad hoc changes. Control in these systems is aggregated at higher levels, as opposed to distributed control spread out through the system. This centralization of control limits the adaptability of systems by removing the ability of components to act independently in the face of changing conditions. Once the system is disrupted or centralized controls are undermined, the system breaks down.[27]

The combination of these two system features—tight coupling and complexity—*together* creates normal accidents. Put these two features

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

together and the system is prone to fail. Even small disruptions can spiral into system failures. Under these conditions, unexpected interactions are the norm (thanks to complexity), and failures, when they inevitably happen, will quickly multiply (there is little time to improvise or limit the failure in a tightly coupled system). Underlying Perrow's discussion of linear/complex and loose/tightly coupled systems is an antipathy toward dependencies and the accumulation of power. Perrow sees increasing dependence both within and between systems, inter- and intradependencies, as offering new possibilities for failure.[28] The benefits of increasing complexity and tightly coupled systems are, in some cases, plain: they need less space, require fewer resources, and appear, if the costs and consequences of failure are ignored or overlooked, to be more economically efficient.[29] Yet they imperil the ability of systems to absorb the shocks of small failures and, instead, create conditions conducive to systemic failure.

Normal accident theory will reappear in the following pages. It is an elastic framework: it is a general "theory of systems" that can be used to examine disparate systems.[30] It provides a useful yardstick to measure the ongoing organization and reorganization of the postal system, freight rail network, and electric power grid. Perrow's framework is inherently qualitative; it is not a rigid formula for diagnosing resilience and vulnerability but rather provides a useful working vocabulary to examine different systems and their changes over time. It is important to bear in mind that these categories—the space between linear and complex, loose and tight coupling—are distinctions of degree.[31] Yet the consequences of where on this sliding scale a system falls are significant; the distinction can mean the difference between an accident and a catastrophe, a local emergency and a national crisis, and a resilient system and one primed to fail.

A close look at the postal system, freight rail network, and electric power system in this and the next chapter can serve to fix these infrastructures on a plot between linear and complex and between tight and loosely coupled. Normal accident theory offers a way of making sense of how these systems change over time. The structure of regulation helped build systems that were both linear and loosely coupled. In time, political changes—deregulation—would transform these systems into tightly coupled and complex constellations. But, these changes were anything but inevitable. It was concrete political choices that helped build these systems. And it would be political choices, and not technological inevitability, that would later remake these systems.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The Postal System: Regulation and Distributed Control

Regulation took different forms and shaped in different ways the postal system, the freight rail network, and the electric power system. In each case the specific regulatory apparatus became drilled into the guts of the infrastructure. The regulation of the postal system supported a network structure characterized by linear processing and loose coupling. It promoted dispersed control—labor-intensive information processing and control spread throughout the network—and worked against the widespread adoption of technologies, such as mechanization and automation, that would have increased complexity and tight coupling. This structure grew out of a particular model of postal governance. The congressional oversight of postal rates and budget favored short-term planning and fixes at the expense of long-term projects and investments. As a consequence the regulatory structure restrained modernization efforts seeking to remake the postal network. The structure of regulation obstructed the Post Office's investment in research and development and the acquisition of new sorting and processing technologies that would eliminate distributed processing, cut the cost of processing the mail, and increase throughput. It instead supported increasingly adding armies of postal clerks to sort and process the mail throughout the network. This might not have been the most economically efficient approach, but it added a measure of resilience into the network. In this fashion the architecture of the network embodied the structure and particularity of postal regulations: the outlines of the network—its vagaries of form and durable oddities—reflected the structure of regulation.

The support for resilience was a side effect of a regulatory regime that supported other sets of benefits and aims. This would also be the case in freight rail and electric power. First and foremost, regulation sought to strike a compromise between different infrastructure publics and offer a means to make these diverse interests heard. The postal system was accountable to these different publics most plainly through congressional control. Congress worked to benefit, at different moments in different ways, a range of publics, including rural communities and urban letter writers, newspapers and public officials, political parties and postal workers. Sometimes the different interests of these groups aligned; sometimes their interests diverged. Time and again, public control over the postal system enacted accommodations and imperfect compromises between these publics. The concreate outcome of regulation was the promotion of a range of public goals often in direct opposition to what the market would

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

otherwise support. Postal regulation undergirded a thriving national arena of communication and commerce.[32] It designed into the system of rates and classifications broad support for public information—newspapers, magazines, and the correspondence of public officials, most prominently—and it extended service across the nation, even when mail volume would not sustain it.[33] The arrival of cheap letter postage during the middle decades of the 19th century helped spark new forms of popular sociability and was a boon for businesses.[34] At every turn, governmental control shaped the contours of the print economy in ways that were at odds with market forces. The pursuit of these other goals incidentally supported a loosely coupled and linear system.

National Operation as Regulation: The Structure of Postal Regulation

In the United States, postal service, unlike other network infrastructures, developed as a state-run enterprise. Unlike the private systems of rail and electric power, the postal system was not subject to oversight by an independent regulatory commission. It was directly operated by the federal government through the Post Office Department.[35] State stewardship of the postal communication was not novel. During the 18th century, it was common for nations to directly control postal communication through an arm of the state. In this tradition, Article 1, Section 8 of the Constitution reserved for Congress "the Power … to establish Post Offices and post Roads."[36] The landmark Postal Act of 1792 defined the hallmarks of U.S. postal policy.[37] The act established a new structure of rates benefiting public information. Low rates and cross-subsidies supported newspapers and the exchange of information about public affairs. Importantly, the act codified the congressional role in establishing new routes. This move was incredibly consequential. It all but ensured that the U.S. postal system would expand across the nation, regardless of revenue and cost consideration.[38] Congress served a geographically diverse constituency, and the postal system would do the same. Giving Congress, and not the executive branch, the power to determine the scope of the system made the granting of new routes and extensions to new rural areas a mere formality.[39] State control was typical of the period, but these changes—this particular use of state power—was radical. It treated the postal system as an adjunct of public life and not as a source of general state revenue or punitive state power. With the Postal Act of 1792, U.S. postal policy sparked what historian Richard John identifies as a "communications revolution" within antebellum America. It led to the wide distribution of public information and the extension of service across the nation.[40] This

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

model of control over the postal economy was driven by political considerations and institutional decisions. Both Federalists and Jeffersonian Republicans supported the new emphasis: Federalists saw it as a useful tool for sowing the bonds of national community across a geographically expansive area; Republicans saw it as a means of keeping tabs on the workings of the remote central government.[41] But the full magnitude of the changes that this new model of postal communication would unleash was not necessarily clear in 1792. In time, however, its transformative effect—the creation of a system that connected communities small and large into a web of communication and commerce—would become plain.

Though postal service operated under a different institutional structure than other regulated infrastructures, in this case state operation and regulation ultimately functioned in a similar fashion. Indeed, public operation functioned as a type of regulation: it controlled rates not through the market but through administrative processes (in this case congressional deliberations) that were open to different publics; it limited competition within a defined sector of the economy; legal monopoly protections supported cross-subsidies in support of the public good, here defined as support for service that was national in scope (greatly benefiting rural areas that were not otherwise economically viable) and discounts for public information; and the Post Office Department retained some power to define, enforce, and adjudicate complaints regarding rules of service.[42]

Power to oversee the operation of the Post Office was split between the executive branch and Congress. The president played a key role in the operation of the post office through the appointment of the top staff of the Post Office Department—the postmaster general, deputy postmaster general, and assistant postmasters general—and through the appointment of local postmasters. The postmaster general was a key political appointee and served as a member of the cabinet between 1829 and reorganization in the 1970s. Control over the postal bureaucracy was a useful way of rewarding key constituents. The appointment of local postmasters was a key source of political patronage.[43] But Congress had a vital role as well. The scope of the postal monopoly and the terms in which private firms could engage in postal services were fixed by federal law under the Private Express Statutes.[44] The postal monopoly, generally, only extended to prevent the for-profit routine carriage of letters over postal routes and functioned as a revenue-protection measure to ensure financing for the postal system as a whole and the maintenance of cross-subsidies for valued forms of content.[45] Crucially, Congress held the power to define the establishment and extension of routes, determine the scope of the postal

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

network, establish different classes of mail, set wages for employees, and fix rates for the various classes. Congress regularly used this power to rapidly expand the postal network and keep rates exceedingly low, at first favoring public information (newspapers and other documents relating to public affairs) with low rates and later subsidizing personal communication through cheap rates for letters. Congress also exerted direct control over the operation of postal service through the appropriations process. Once annual appropriations to offset postal deficits became common and central to postal revenue after the 1820s (see below), the role of Congress in postal affairs greatly expanded. Congress held tight control over the operations and accounts of the Post Office Department; the Post Office was compelled to seek approval for large projects and undertakings.[46] Through the appropriations process, Congress reviewed and controlled all major capital outlays and used this power to, in effect, set the budget for the department. In these ways, Congress set the basic terms of service for the postal system and controlled key elements of cost (including the scope of service and compensation), revenue (through the fixing of rates), and operations (through control over the postal budget).

Congressional Control, Information and Communication Technologies, and Network Organization

Postal regulation before the beginning of sweeping reform in 1970 subsidized a network that, seen through a narrow lens, contained structural inefficiencies. It propped up a network that favored labor and distributed processing over technology and consolidation. This was not the most efficient model. Seen from a slightly different angle, postal regulation supported a loosely coupled and linear network. Between World War II and 1970, the Post Office lagged behind other large-scale, labor-intensive operations in terms of adopting new technologies and instead relied on increasing labor to offset growing postal volume. While comparable industries and firms adopted new mechanized and, later, automated technologies, the postal system continued operating as it had for nearly a century, relying on hand processing and an army of trained clerks to continually route and sort the mail as it passed through the network. The continuation and durability of antiquated methods of processing and distributing the mail were linked to the broader structure within which the postal system operated. The Post Office did not have the resources needed to pursue the widespread adoption of new information and communication technologies (ICTs) that would consolidate and streamline the postal network. As in other infrastructures, the material structure of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Figure 1.1
Clerks and carriers in a large city post office. Image courtesy of the Smithsonian Institution, National Postal Museum.

the network embodied the particular regulatory regime under which it operated.

In the century before regulatory reform, the work of sorting and processing the mail changed remarkably little. Clerks and carriers situated throughout the postal network routed and sorted the mail repeatedly by hand based on complicated memorized "schemes" delineating postal routes and transit points (see figure 1.1). Other options were available. The Post Office initially tested mechanized equipment for handling and sorting the mail in the 1920s, and such equipment was readily available by the 1950s; automated equipment became available during the mid-1960s.[47] Yet postal workers remained largely unaided by mechanical or automated equipment before reorganization in 1970; rather, they processed letters by hand and sorted mail by adopting the "peek-and-poke" method, "peeking" at the address then "poking" letters into designated bins or cases for transfer based on memorized schemes. The President's Commission on Postal Organization, charged with reviewing postal operation, observed in 1968:

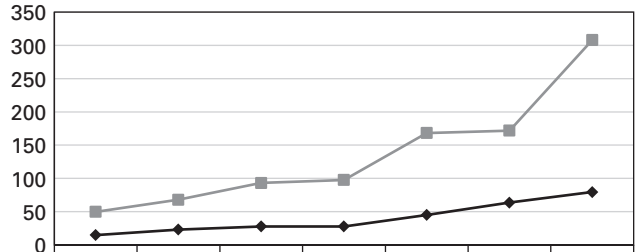
Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

> In most offices men and women lift, haul and push mail sacks and boxes with little more mechanical assistance than the handcart available centuries ago. In the electronic era, the basic sorting device remains the pigeonhole case into which letters are placed, by hand, one by one. The basic parcel post container is the canvas sack, filled, lifted and "dumped" by human labor … the Post Office relies almost totally upon human labor for bulk materials handling and distribution—the transfer of mail between work stations, and the loading and unloading of vehicles.[48]

In 1969, a year before the passage of significant reforms, a stunning 90% of all mail was still processed by hand, and fewer than 5% of the largest 300 postal facilities were mechanized.[49] The average letter traveling through the postal network was sorted and re-sorted between 10 and 18 times, in five to six different post offices, before reaching its destination.[50] The system's backbone comprised 552 sectional sorting centers, large facilities linked by air routes, connecting regional, city, and branch post offices.[51] In manual sorting, clerks and carriers performed informational work based on memorized data sets. This was linear, rather than complex, work. Clerks routed mail to the next step in the sequence in an assembly-line model of sorting. Clerks at different offices sorted mail into increasingly fine-grained categories until it eventually wound up at its destination. Under this model, processing was spread across a number of postal hubs. The reliance on workers' manual ability and memorization of information for routing and sorting limited throughput and the number of distribution points that any single facility could serve.[52] Manual sorting placed a limit on the centralization of control. This was not only a linear model; it was also loosely coupled. The postal system could be slowed down without breaking the entire system. The various nodes in the network operated with some degree of independence. If one failed, it would have downstream impacts, but other complementary offices could continue to operate and route around the failure until the affected office came back online. There was a degree of flexibility or independence within individual offices that would disappear with automation and mechanization. The postal system as it stood before the 1970s was a near-perfect approximation of a linear and loosely coupled system.

As the postal system continued to rely on antiquated methods to process the mail, the volume of mail continued to rise. The Post Office Department confronted spikes in volume, particularly the sharp increase post–World War II, by adding clerks to the rolls in increasing numbers. As postal volume grew sharply throughout the 20th century, so, too, did the number of clerks employed to sort the mail (see figure 1.2). Between 1940

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024



	1910	1920	1930	1940	1950	1960	1968
Total mail volume (billions)	14.8	23	27.8	27.7	45	63.6	79.5
Clerks (thousands)	49.8	68	93.2	97.6	168.2	171.9	308.1

Figure 1.2
Post Office mail volume and clerks employed, 1910–1968. Mail volume is not available for 1920; data from 1923 is substituted in the chart. Data from POD, *Annual Report of the Postmaster General, 1969*, 236–241, table 801; and President's Commission on Postal Organization, *Towards Postal Excellence: The Report of the President's Commission on Postal Organization*, 16, 170.

and 1968, both total mail volume and clerks employed roughly tripled: total volume jumped from 27.7 billion to 79.5 billion pieces while clerks employed rose from 97,000 to 308,000.[53] The increase in clerks far outpaced total growth in postal labor. In 1930, clerks accounted for 27% of total workers; by 1968, clerks, the central figures in routing and sorting the mail, accounted for 42% of the total postal workforce. Between 1930 and 1968, total nonclerk postal labor increased by 71.6%, while clerks over the same period increased by 230.5% (see figure 1.3).[54]

New equipment that became available during the 1950s and 1960s held out the prospect of radically reordering how the postal system operated. Mechanization and automation offered the possibility of cutting costs and improving efficiency. These technologies could reduce labor costs and concentrate the sorting and processing of mail in a few large centralized hubs (in order to capture the benefits afforded by economies of scale). New technology offered the possibility of largely deskilling the process of sorting and processing the mail while expanding throughput and decreasing unit costs.[55] Mechanized and automated equipment could simplify the work of clerks by reducing the cognitive burdens associated with sorting the mail. By embedding such knowledge in the equipment, a rotating cast of comparatively deskilled (and cheaper) workers could ably complete the same tasks. By the 1960s, mechanized and automated equipment offered significant savings: mechanized equipment used in culling, stacking, and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

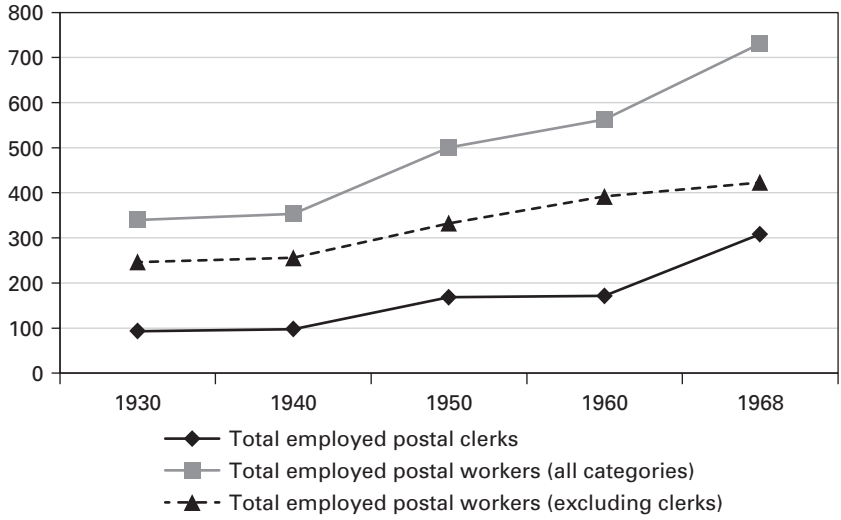


Figure 1.3
Postal employment, 1930–1968. Data from President's Commission on Postal Organization, *Towards Postal Excellence: The Report of the President's Commission on Postal Organization*, 16, 170; and POD, *Annual Report of the Postmaster General, 1969*, 246, table 804.

canceling mail cost $1.20 per thousand letters, compared against $3.50 per thousand for manual processes; automated processing and sorting operated at $2.00 per thousand letters, mechanized equipment operated at $3.42 per thousand letters, and manual sorting and processing cost $4.20 per thousand letters.[56] The difference in throughput reveals similar disparities. The average clerk processed 600 letters per hour, workers aided by mechanization averaged 2,800 letters per hour, and automated equipment processed 30,000 letters per hour.[57] Additionally, mechanized and automated equipment allowed mail to be sorted into a greater number of divisions. Before mechanization, clerks sorted mail into 55 distinct separations, while mechanized equipment allowed for 277 divisions and eliminated the need for multiple sorts throughout the network.[58]

Adopting these technologies would have directly cut against the system's loosely coupled and linear organization. This potential shift—from manual sorting to mechanized and automated—would add new complexity into the network. Manual sorting was a sequential affair, a linear, step-by-step process that moved mail from office to office. Mechanization and automation sought to cut out these steps, as mail would be sorted in large facilities with minimal additional sorting. This increased the complexity of sorting significantly. The sequential sorting of the mail would

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

be replaced by automated machines that sorted mail only once or twice before delivery.

The savings made possible by expensive mechanized and automated equipment through economies of scale could only be captured by reorganizing the internal network-processing centers into a small number of core facilities. This would work to transform the postal network into a tightly coupled system. Machination and automation would only pay off if large volumes of mail were aggregated within a small number of centralized processing centers.[59] Mechanization and automation held out the tantalizing possibility of slashing costs and creating a newly efficient postal network that was tightly coupled and complex, linking a small number of massive automated distribution and processing centers that sorted and prepared mail for the entire network. Such a system might be cheaper, but it would be inflexible. Processing and distribution centers could not be slowed down or replaced without seriously fouling up the entire network. Under this approach, an increasing range of homes, businesses, and postal customers would rely on a few dense postal hubs for the processing of their mail. These new dense hubs, if created, would become new single points of failure within the network.

The regulatory structure governing the postal system, however, actively frustrated the widespread adoption of these new technologies.[60] At the most general level, the postal model of monopoly protection and deficit financing through annual appropriation buffered the Post Office Department from competitive pressures. The Post Office had a legally guaranteed market and received annual appropriations to offset shortfalls. This somewhat reduced the incentives faced by management to pursue the most cost-effective means of processing the mail. Appropriations became common after the 1820s and offset roughly 15% of total postal costs in the following decades.[61] In the late 1960s, a presidential commission formed to study the postal system drew an explicit connection between the appropriations and inefficiencies, remarking that "the practice of making up losses from the Federal Treasury removes much of the incentive for efficient operation. There is no need to control costs if a supplemental appropriation may be expected as a matter of course."[62] While public pressure historically pushed the Post Office to innovate in providing new services for consumers, like rural free delivery, a comparable movement to push the Post Office to pursue internal improvements did not develop; mechanization and automation were "back of the house" issues that did not directly touch the experience of the mailing public. The incentives to innovate to reduce operating costs were somewhat muted.[63]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

By the 1950s and early 1960s, however, postal management actively sought to reduce costs through innovating and transforming the postal network using mechanization and automation. Repeatedly, in annual reports and congressional testimony, the postmaster general underlined the importance of investing in new technology and called for a strong commitment to support postal efforts to implement *postal modernization*, a phrase synonymous with mechanization and automation.[64] The lack of innovation, then, was neither entirely, or perhaps even centrally, a question of missing incentives or will on the part of postal management nor a side effect of a lazy monopolist or complacent public agency. Rather, the lack of innovation was directly tied to the congressional role in postal finances. Congress controlled postal finances both by setting rates and, more importantly, by controlling the postal budget through the appropriations process.

Historically, postal rates under congressional control stayed flat and did not rise to meet expanding costs. Once established, rates developed an inertia that was difficult to dislodge: Congress was loath to undertake the unpopular and highly visible step of passing legislation increasing postal rates, and the industries reliant on cheap postage to distribute books, magazines, catalogs, and other goods actively lobbied for their continuation at the expense of growing revenue shortfalls.[65] For its part, the Post Office, too, was sensitive to the political machinations required to raise rates and would frequently refrain from requesting a general rate increase during an election year or in close succession with a previous rate hike, regardless of actual need.[66] As a result, postal rates did not rise to keep pace with the rising postal deficit. For example, first-class postage was only adjusted seven times in the 100 years before 1968, while the majority of all second-class mailings traveled at rates of less than two cents in 1968, roughly the same rate they would have been charged *a century earlier*.[67] Costs played a minor role in establishing postal rates, and they were routinely ignored—trumped by politics—during the legislative process (see figures 1.4 and 1.5).[68]

Most significantly, Congress wielded the appropriations process to exert tight control over how the Post Office allocated its resources. The Post Office Department, unlike private industry, did not have discretionary authority over how it spent its revenue. Each year the revenue collected by the Post Office through rates was deposited into the federal treasury. At the end of the year, Congress appropriated the collected revenue, along with an additional sum to close the accumulated yearly deficit, back to the Post Office Department. This appropriation came with strings attached.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

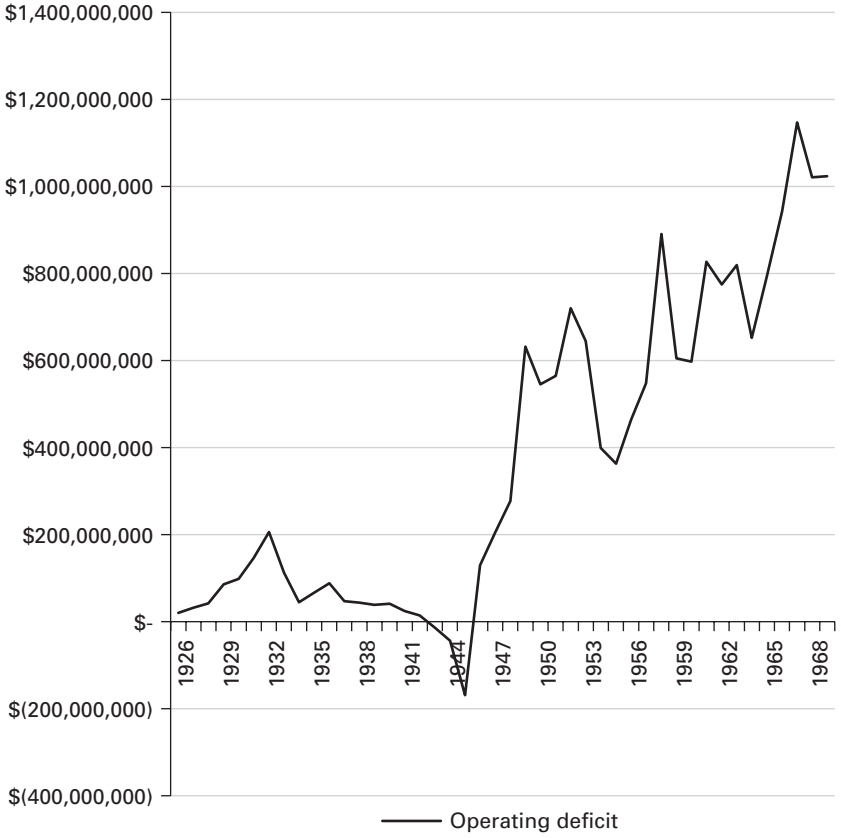


Figure 1.4
Postal operating deficit, 1926–1969. The operating deficit represents expense over income. For an explanation of how the postal deficit is calculated, see POD, *Annual Report of the Postmaster General, 1969*, 166–168. Table data collected from ibid., 236–241, table 801.

Congress included binding limits on how these funds were to be used. Complicating matters even more, control over the different aspects of postal finances—the setting of rates and the crafting of appropriations—was fractured among different congressional committees with little coordination: the House and Senate Committees on the Post Office and Civil Service set postal rates, but the Appropriations Committees allocated funds for the Post Office.[69] This system of congressional control worked to keep the postal system afloat, but it starved it of the capital needed to engage in postal modernization by keeping rates low and by refusing to provide appropriations to cover expensive, long-term investments.[70]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

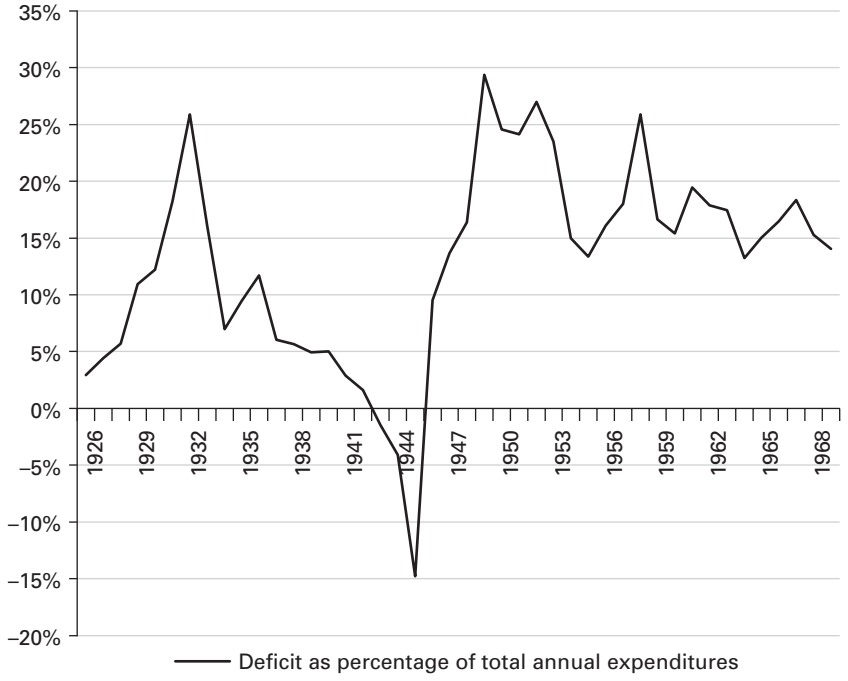


Figure 1.5
Postal deficit as a percentage of total annual postal expenditures, 1926–1969. All table data collected from POD, *Annual Report of the Postmaster General, 1969*, 236–241, table 801.

This process gave Congress enormous power over postal spending. Congress reviewed major proposed projects and appropriated the postal budget into eight different categories (see table 1.1) between which the Post Office could not, by penalty of law, transfer funds.[71] Though appropriations rose above total revenue to offset the deficit, the drain imposed on postal finances due to low rates did have a real impact on total funds available and, consequently, efforts to modernize. The Appropriations Committees used collected revenue as a baseline when determining the total amount of funds to appropriate and attempted to limit, to the greatest extent possible, the level of appropriated funds above collected revenue.[72] In defining the postal budget, Congress routinely pursued a strategy of incremental increases in funds—minor year-to-year increases—as opposed to major new allocations. The Post Office held a legal monopoly that granted it nearly complete market control, yet, by virtue of congressional control over rates and budget, it had a paucity of resources to invest in internal improvements.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Table 1.1
Post Office Department appropriation categories.

Appropriation	Description
1. Administration and Regional Operations	• Headquarters administration • Field inspection service • Regional operation • Postal data centers
2. Research, Development, and Engineering	• Direct operation • Engineering support services • Contract research and development
3. Operations	• Administration of postal installations • Labor (postmasters, supervisors, clerks, carriers, mailhandlers) • Maintenance service • Vehicle service
4. Transportation	• Surface and air transportation
5. Building Occupancy	• Rent • Fuel • Site acquisition
6. Postal Supplies	• Supplies and services
7. Plant and Equipment	• Federal building improvements • Vehicles • Mail processing equipment • Postal support equipment
8. Postal Public Buildings	• Sites, design, and expenses • Construction

Source: Condensed from Little, "Description of the Postal Service," 6–35, table 6.3.4.

In reviewing postal expenditures, Congress concerned itself most centrally with figures associated with inputs and cost data, at the expense of more thorough studies of output and efficiency.[73] The irony was rich. In setting prices, Congress cared little for how much the service actually cost, but when it came time to consider expenditures, short-term costs were, in effect, all that mattered. As a result, appropriations were overwhelmingly assigned to operations, labor, and other day-to-day costs while all but ignoring investments in long-term capital projects, such as building new postal facilities, acquiring new equipment, or investment in research and development that offered up-front outlays and delayed benefits. The refusal of Congress to provide such funds reflects both the general challenges associated with the decision-making of elected public officials

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

concerning projects with long-term benefits, as well as circumstances unique to the Post Office. Congressional reluctance to look beyond the narrow exigencies of the moment and engage in long-term planning stems in part from the familiar disjunction of time horizons confronting members of Congress and the benefits of long-term investment. Members of Congress faced the immediate pressure to maintain postal service *and* to limit federal postal spending relative to other pressing national needs. Investing in R&D (research and development) and new postal technology, however, only yields gains in later years—as investments eventually reduce unit costs and take a bite out of postal expenses—when the members of Congress that initially supported the investment would perhaps be out of office.[74] But these general challenges were greatly inflamed by dividing the authority for rates and the budget between two different sets of committees—the split between the Post Office and Civil Service Committees and the Appropriations Committees all but guaranteed that short-term decisions would trump long-term planning. At the same time, postal labor, a significant and well-organized interest group, actively lobbied against investment in new technology.[75] Though labor publicly supported the aims of mechanization and automation, behind the scenes they moved to obstruct the process in order to prevent job reductions.[76]

The figures concerning Post Office investment in developing new technologies and funding large capital projects under congressional control are telling. After World War II, the Post Office created a Research and Development Bureau to help spur innovation. Yet, even after the beginning of R&D spending in 1950, funding remained nearly microscopic relative to the size of postal operations. Between 1950 and 1970 (before reorganization), the Post Office, at the instruction of Congress, invested an average of .17% of the total postal budget on R&D. During this time the Post Office never invested more than .47% of its total obligations in R&D in any single year (see figures 1.6 and 1.7). Postal investment in large capital projects followed a similar, if slightly less dramatic, outline. Between 1955, when efforts to modernize got off the ground, and 1968, Congress set aside only $520 million for the Post Office to apply to large capital projects (including mechanization, automation, and new facility construction), an average of 1.16% of total obligations to large capital projects per year (see figures 1.8 and 1.9). In nine of those years, investment in capital projects fell below 1% of total obligations. Nearly two-thirds of this spending was devoted to creating new postal facilities, while the remaining one-third was spent on mechanization projects.[77] As a result, the Post Office at the end of the 1960s fell well behind private

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

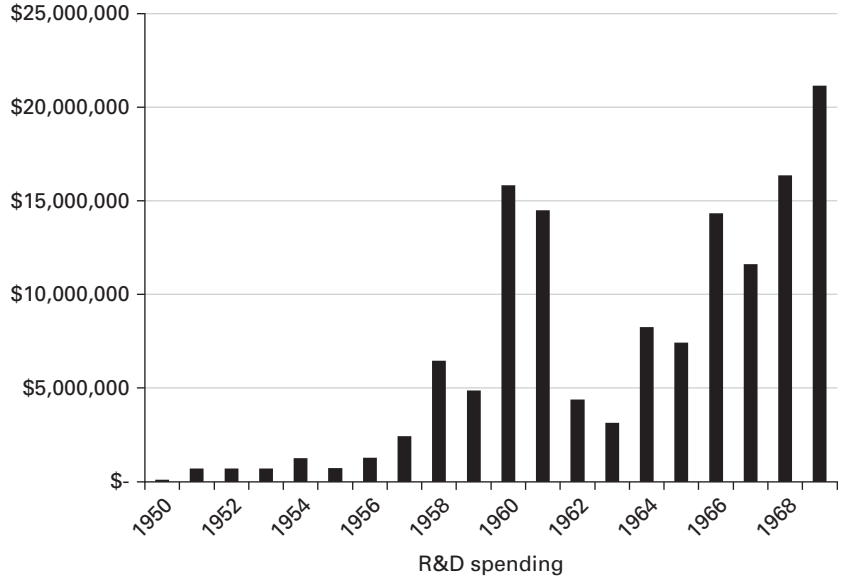


Figure 1.6
Post Office research and development spending, 1950–1969. POD, *Annual Report of the Postmaster General, 1969*, 246, table 804.

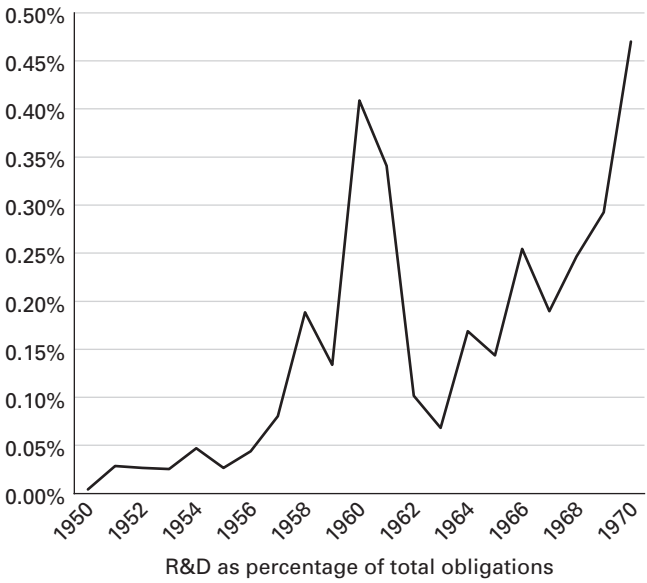


Figure 1.7
Percentage of total postal obligations devoted to research and development, 1950–1970. POD, *Annual Report of the Postmaster General, 1969*, 246, table 804; Mustafa, *Postal Technology and Management*, 35.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

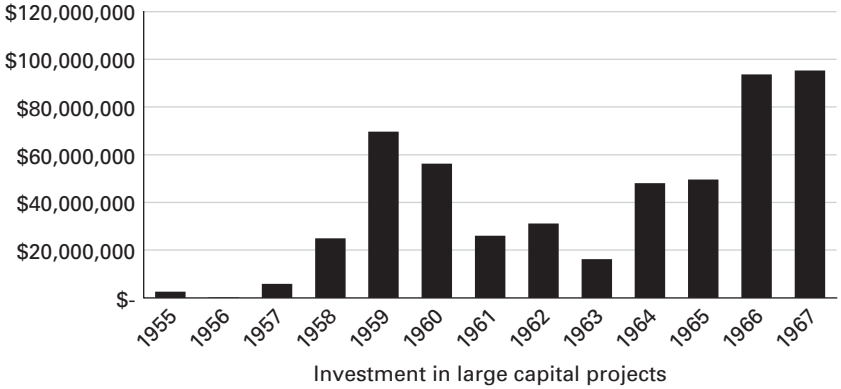


Figure 1.8
Annual postal investment in large capital projects, 1955–1967. In accounting, the Post Office divided large capital expenditures into three categories: land and buildings, fixed mechanization, and nonfixed mechanization. Fixed mechanization included equipment that was facility-specific and involved in materials handling, such as conveyor belt systems and sack-sorting systems. Nonfixed equipment was defined as equipment used in processing the mail and that could be used across facilities. Included were letter-sorting machines, facer cancelers, and stacker feeders, as well as other pieces. Little, "Description of the Postal Service," 4-19-4-20.

industry in terms of assets per employee. By 1968 the Post Office Department had roughly an asset-per-employee ratio of $700 ($700 in assets for each employee), while Fortune's 500 largest industrials had a minimum asset-per-employee ratio of $5,760.[78] Firms with a similar degree of labor intensity, such as merchandizing firms and the transportation firm Consolidated Freightways, had an asset-per-employee ratio between $4,000 and $5,000. According to any measure, postal investment in capital projects lagged seriously behind comparable enterprises.[79] In 1968 the Post Office and the President's Commission on Postal Organization estimated that a new investment of $5 billion—10 times the amount invested in the past 13 years—was needed to make up for chronic underinvestment.[80]

Regulation and Network Structure: The Post Office

Congressional control molded the larger structure of the postal network. The broader regulatory structure governing the postal system was valuable in providing a national market for communication, subsidizing the diffusion of news and information, and undergirding the integration of rural communities into the life of the nation (as well as other goals). But congressional control over finances served as a barrier to the widespread adoption of new technologies that could reduce costs and transform

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

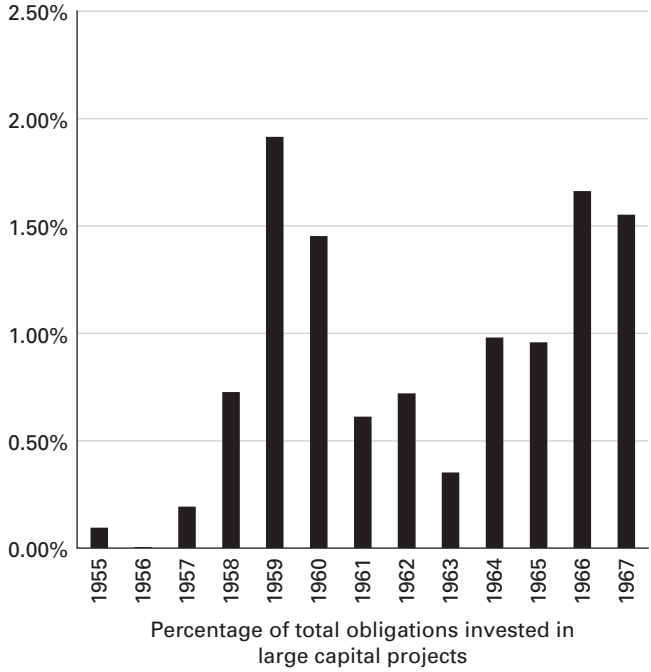


Figure 1.9
Percentage of postal obligations devoted to large capital projects, 1955–1967. Little, "Description of the Postal Service," 4–23, table 4.1.10; POD, *Annual Report of the Postmaster General, 1969*, 246, table 804.

control within the network. The lack of innovation in new technologies of automation and mechanization, or postal modernization, as it was described during the 1950s and 1960s, was not a failing of postal management per se but rather a side effect of congressional control.

There was, however, a silver lining. Inefficiency has its benefits. Etched into the historic James A. Farley post office building in New York City is the famous translation from Herodotus: "Neither snow nor rain nor heat nor gloom of night stays these couriers from the swift completion of their appointed rounds."[81] The quotation serves as a well-known unofficial motto for the Post Office. Yet, while the endurance and valor of postal workers is often praised, it is worth noting that far less heralded structural forces—forces that by the 1950s and 1960s were explicitly understood by Post Office Department management to be problems in need of fixing—also contributed to the resilience of the postal system. Postal regulation supported loose coupling and linearity. By favoring labor over new technologies, regulation buttressed a network where control was distributed.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The distribution of processing throughout the network meant that disruptions were local. A snow storm in Boston, a flood in New York, or an earthquake in Los Angeles might disrupt mail delivery and processing on a local level, but these disruptions would be limited and constrained. These sorts of incidents did not have system-wide consequences. A local disruption was just that—a local disruption.[82] The network was loosely coupled and linear—processing and reprocessing continually occurred as mail moved through the system: individual failures could be routed around and isolated. This model was certainly not cheap or the most efficient, but it did provide a network structure that was resilient.

Regulating the Railroads: Redundancy and the Unintended Benefits of Rate Policy

Few industries were as powerful as the railroads during the 19th century. They seemed to hold the fate of towns, cities, and entire industries in the palm of their hands. Yet chronic instability jeopardized key rail lines and led to cycles of boom and bust. Railroad regulation, once it arrived, was a salve (albeit an imperfect one). Price-and-entry regulation grew out of the late-19th-century efforts of key shippers and civic groups to check the new, then virtually unrivaled, power of the railroads over the terms of the economy and the agitation of the railroads themselves to limit ruinous competition within the industry. The intersection of divergent infrastructure publics led to the creation of the Interstate Commerce Commission (ICC), the first modern regulatory agency, in 1887 and the mechanisms of regulation that stood in place for nearly 90 years. Regulation prevented the most egregious forms of monopoly abuse and stabilized the industry by preventing destructive competition in the form of rate wars, rebates, and drawbacks. The regulation of freight rail also provided an unexpected benefit: it served as a de facto tax on dangerous bulk shipments of hazardous materials. This was very much an unintended side effect of regulation. The ICC's approach to rate design helped reduce the transportation of bulk shipments of hazardous materials via rail. At the same time, regulatory control over rates, abandonments, and mergers underwrote an expansive and redundant rail network. This, too, had real benefits to safety and security. An expansive network made it possible to direct hazardous shipments across routes that avoided dense areas. In this fashion, the regulation of freight railroads provided a hedge against catastrophic failure: it worked to systematically limit the shipment of large batches of dangerous chemicals through urban areas.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

State Support and Subsidy: Early Railroad Growth and Development

Government involvement in U.S. railroads predates federal regulation. Indeed, it is difficult to find a moment when the state was not engaged with the railroads.[83] Before the American Civil War, the states and federal government played a key role in fostering the development and growth of railroads in an effort to link local communities with expanding markets of trade and spur commerce.[84] Merchants and shippers called for direct public subsidies in support of the new emerging system of transportation.[85] Direct public subsidies to private railroads, particularly before the 1860s, were a key source of capital.[86] Additionally, growing rail networks benefited from public support by using eminent domain law to provide rights-of-way and the proffering of lucrative mail contracts.[87] After modest development in the 1830s, the railroad boom that began in the middle of the 1840s brought rapid expansion first to New England and then the South and the West. By 1854 the main intersectional trunk lines—the Erie, the Baltimore and Ohio, the Pennsylvania, and the New York Central—provided links between the East and West.[88] During the middle decades of the 19th century, railroads grew steadily (see figure 1.10) and included nearly 100,000 miles of track by 1880.

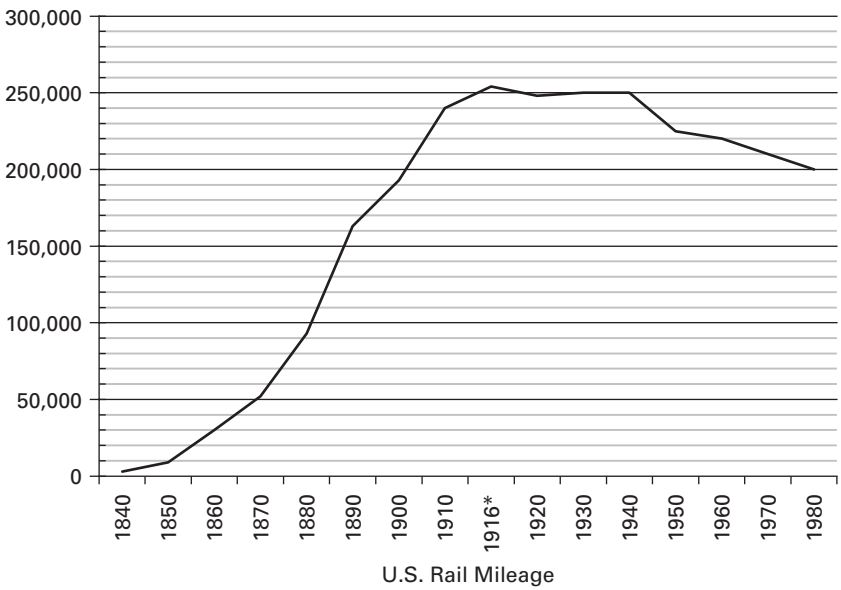


Figure 1.10
U.S. rail mileage, 1840–1920. Peak mileage was in 1916. Information drawn from Chandler, *Visible Hand*, 82–83, 89; Rodrigue, Comtois, and Slack, *Geography of Transport Systems*.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The Need for Regulation: Monopoly Power and Ruinous Competition

It is difficult to overstate the transformative impact of railroads on 19th-century America. Railroads reordered established, and mainly local, patterns of trade and fed the growth of a national market dominated by forms of mass distribution and production.[89] They provided a new unparalleled locus of power in American life; railroads could, through the setting of rates and terms of access, determine the entire fortunes of a city or region. On some lines, railroads operated as a monopoly and, as a result, wielded incredible power to control markets for goods.[90] Even in markets with modest competition, skewed rates that benefited certain producers or shippers over others could elevate and impoverish in equal measures.[91] The rush to use public funds and grant rights-of-way to support the railroads was initially an attempt by local communities to secure the benefits afforded by rail transportation and was, in some cases, seen as a matter of survival.[92] Yet once the railroads arrived, discriminatory practices offered bitter frustration. After raising funds to attract service, the promise of cheap access to markets often proved to be an illusion. Shippers, including farmers, merchants, and independent oil producers, viewed these practices as violations of basic notions of fair play.[93] Their grievances were legion. Popular discontent by famers toward the railroads led the Granger movement to adopt rail reform as a cornerstone of their activities. Merchants in New York City pushed for rail regulation as a way of checking the power of the railroads over their fortunes. The vagaries of rail rates, in their eyes, favored other locals—notably, Boston and Baltimore—over New York. Independent oil producers also pushed for regulations as a way of injecting some equality into a system of rates that favored the dominance of Standard Oil. These (and other) infrastructure publics agitated for regulation as a way of making these powerful networks publicly accountable.

Shipping interests were not alone in seeking regulation as a palliative to the new problems introduced by the growth of the rail networks: the railroads, too, sought regulation. Here, the problem was not too little competition but too much: competition in areas with multiple lines proved to be ruinous. In a seeming paradox, the railroads faced both too little and too much competition. As Ari and Olive Hoogenboom note, "Railroads were the first large American business and were absolute monopolies in large areas, yet fiercely competitive at many points."[94] Through lines and segments connecting urban centers were often served by multiple railroads. Railroads are characterized by high fixed costs, and the pressure to secure high volume through low rates to defray those costs was often difficult to ignore.[95] On competitive lines, railroads engaged in periodic rate wars,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

sending rates downward, and offered large users generous benefits in the form of rebates and drawbacks—fees that railroads charged to particular shippers of a certain commodity that were then paid to other more powerful shippers of the same commodity in an effort to court traffic and secure market share.[96] As a result, maintaining profitability on competitive lines proved difficult, and major railroads frequently faced bankruptcy. To combat the destructive effects of competition, railroads first turned toward voluntary associations—formal and informal pools and rate agreements to fix rates at certain levels (and prevent drawbacks and secret rebates), divide traffic among pool members, and share revenue—and later, during the 1880s, undertook massive campaigns to build larger end-to-end networks in an attempt to secure steady streams of traffic and eliminate competition (see figure 1.10).[97] Neither strategy succeeded. Voluntary agreements were not legally binding, and members broke agreements when it suited their interests, dissolving the pools. Additionally, enlarged end-to-end networks failed to eliminate competition.[98]

The Interstate Commerce Commission: Regulating the Railroads

Initially, states attempted to impose control over railroad operations through charters and state commissions—an approach that would also be tried with electric power. These efforts proved to be ineffective.[99] Federal control would be needed. The Supreme Court considered the legality of state controls over the railroads (and other infrastructural services) in the landmark case of *Munn v. Illinois* (1876). They affirmed the contention, long established as a part of English common law, that certain types of private enterprises, *common callings* or *common carriers*, are imbued with a public interest due to their importance to commerce or scarcity and, as such, cease to be solely private.[100] In particular, the court reasoned that infrastructure services, such as railroads, are imbued with a larger significance and responsibility because they "stand … in the very 'gateway of commerce'"—that is, they are the infrastructures upon which commerce operates.[101] The railroads, however, easily circumvented state control over rates by adjusting rates on interstate traffic.[102] The final nail in the coffin of state regulation came in *Wabash v. Illinois* (1886), when the Supreme Court struck down interstate rate regulation by individual states as inconsistent with the interstate commerce clause of the Constitution.[103]

In the wake of *Wabash*, Congress passed the Interstate Commerce Act of 1887 and created the ICC to regulate the national railroad system. The act provided a general mandate for the ICC to enforce basic common-carrier principles, including nondiscrimination and fair and reasonable

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

rates, while leaving the ICC room to define how these principles would be translated into practice.[104] Federal regulation offered a compromise between shipping interests and the railroads.[105] The ICC eliminated the worst abuses of monopoly power and provided shippers with access to rail service on predictable, reasonable, and equitable terms. It made the railroads publicly accountable. At the same time, the ICC also clearly served the interests of the railroads: the commission stabilized rates, provided an avenue for collective rate making, ensured a stable rate of return for the railroads, and eliminated the unpredictable nature of regulation by individual states.[106] Like governmental control over the postal system, rail regulation accommodated and struck compromises—compromises that favored some over others to be sure—between different infrastructure publics.

The Interstate Commerce Act created the ICC as an independent regulatory body headed by five commissioners serving staggered terms and provided the commission with a general mandate to enforce common carrier obligations in the public interest.[107] The act charged that railroads must provide nondiscriminatory service, charge just and reasonable rates, adhere to published rates, and limit the use of pools.[108] The ICC operated on a case-by-case basis and had latitude to enact the provisions of the act.[109] What precisely constituted fair and reasonable rates, for example, was an open question.[110] The ICC represented a new mode of federal public authority that melded the various functions of government—executive, legislative, and judicial. Initially, the courts moved to limit the power of the ICC through a series of decisions that struck a near-fatal blow to the ICC and did not benefit either railroads or shippers.[111] In response, Congress passed a series of laws restoring the powers of the commission.[112] By the end of the first decade of the 20th century, the ICC could set and suspend rates, enact binding decisions, engage in direct scrutiny of rail operations, and allow collective or joint rates filed by the railroads.

The ICC provided the railroads with many of the benefits that voluntary associations failed to provide.[113] The ICC stabilized the industry by limiting competition and maintaining rate levels that could support existing operations.[114] Legally binding rates eliminated competition based on price and supplemented the direct control of entry through licensing procedures with indirect control over entry (as new entrants could not employ below-cost pricing as a way of gaining market share).[115] Additionally, by enforcing published rates, the ICC limited the drain, estimated at 10% of revenue before effective ICC regulation, associated with rebates and drawbacks.[116] In determining reasonable rates, the ICC set rates at levels that provided a stable rate of return for the railroads; in the words of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

one commissioner, railroads ought to earn a "living wage" that attracted investment and allowed them to operate comfortably.[117]

The ICC was not, however, simply a channel for railroad interests. On the contrary, regulation also addressed the concerns voiced for decades by shipping interests. The elimination of special generous deals for valued shippers, such as drawbacks and rebates, in deference to published rates created a level playing field for shippers.[118] Most notably, the call for just and reasonable rates and the prohibition of discriminatory service assured that shippers would not face the destructive caprice of the railroads or the wielding of monopoly power on noncompetitive lines. To this end, the ICC capped the upper limit of rates and set comparable rates for the shipment of comparable goods.[119]

Cross-Subsidies, Mergers, Abandonments, and Excess Track: Regulating an Expansive Network

Regulation was ultimately conservative: it sought to maintain the existing scale of the national rail network through limits on abandonments (discontinuation of service), rates, and the encouragement of strategic mergers. Rather than fostering consolidation and the elimination of little-used rail track as some had hoped and suggested, ICC regulations buttressed the expansive network.[120] A combination of factors—including the generous solicitation of local communities, outright speculation, and the push by railroads to create integrated systems during the period before effective regulation—led to the creation of a rail network characterized by overbuilding (see figure 1.10). The sharpest growth of new track occurred during the 1870s and 1880s, when roughly 125,000 miles, or 50% of the eventual peak rail mileage in the United States, was constructed.[121] Contemporary observers noted that only a third of the added track was justified by increased traffic, with the rest redundant.[122] The network peaked in 1916 with 250,000 road miles and declined gradually through the 1970s as the overall share of intercity freight traveling by rail plummeted (see figure 1.10 and figure 1.11).[123] Reviews conducted during the 1970s estimated that roughly 75% to 80% of the nation's rail system was unsupported by traffic.[124]

Regulatory policy propped up this expansive network through its control over abandonments, rates, and mergers. The Transportation Act of 1920 transferred control over abandonments from the states to the ICC. The ICC, as the states did previously, favored the continuation of service over abandonment and obligated railroads to maintain unprofitable services as part of their common carrier duty to operate in the public

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

convenience and necessity.[125] Typically, if *any* party, such as local shippers or rail customers, objected to a service change, the application would be rejected.[126] The abandonment process itself was costly, slow moving, and complex. As a result, railroads rarely attempted to secure abandonments unless success was inevitable and, instead, chose to carry unprofitable services.[127]

Rate regulation worked in concert with control over abandonments to support the maintenance of the existing outlines of the network. Rail rates were not set according to price. Indeed, the ICC interpreted the nondiscriminatory language of the Interstate Commerce Act to mandate that shippers of comparable goods on high- and low-density lines should not be charged different rates. As a practical matter, the ICC effectively used its control over price to enact subsidies between profitable densely trafficked lines and otherwise unprofitable low-density lines.[128] Like the postal system, regulatory control helped sustain a national system.

The ICC also used its control over mergers and traffic patterns to support the continuation of the expansive network. The Transportation Act of 1920 provided the ICC with power to approve mergers between lines. The ICC used this power to join weaker and stronger lines, rather than eliminate excess capacity, and required merged lines to maintain premerger traffic patterns.[129] The policy of maintaining premerger traffic flows was implemented as early as 1922 and formalized in the ICC's ruling in the case *Detroit, Toledo & Ironton R. Co. Control* (1950) as a regulatory standard known as *DT&I conditions*.[130] The imposition of DT&I conditions reflected the agitation of local shippers, labor, and others that worried about the harm that postmerger consolidation would likely bring. The regulatory oversight of mergers and the imposition of DT&I conditions further worked to prevent the outright consolidation of track through mergers and by preventing the diversion of traffic flows to the most efficient routes. Here again, regulations worked to maintain the historic outlines of the network, rather than support the efficient reorganization of the network into a dense web of heavily trafficked lines running between population centers.

An expansive network was, in some ways, loosely coupled. It allowed rail shipments to move through the network in different ways and created various circuits between different points on the network. This sort of overbuilt network has a degree of internal flexibility: the excess of track allows individual rail shipments to travel different routes.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Rate Regulation, Competition, and the Rise of Trucking

While control over abandonments, rates, and mergers supported an expansive network across which freight moved, the ICC's methodology for calculating rates effectively placed a significant markup on particular types of shipments, including hazardous materials. The ICC's approach to setting rates favored particular users and uses of the rail network. Behind the seemingly bland statistical details of rate construction sat substantive judgments about what types of users and uses of the network mattered. The ICC approach to rate design ultimately helped shift a significant share of intercity freight from railroads to trucking companies.

The ICC used what is known as *value-of-service* rather than *cost-of-service* pricing in setting rates. This mattered. This approach shaped the types of commodities carried by rail and reflected the agitation of particular sets of shippers (namely, farmers). Value-of-service pricing inflated rates for expensive goods while keeping prices low for cheap shipments. Value-of-service pricing (in theory) set rates in accordance with demand elasticities. For goods for which demand fluctuated with price changes, rates were kept low; for those goods for which demand did not vary with price, higher rates were imposed. The ICC's rate design reflected the early agitation of farm interests in securing regulatory relief. This approach had the practical effect of setting very low rates for cheap bulk agricultural products and high rates for more expensive manufactured goods. Since transportation costs accounted for a greater percentage of the price for low-cost commodities, demand demonstrated far greater elasticities for these products compared to more expensive goods. In this manner, value-of-service pricing amounted to value-of-commodity pricing in transportation regulation.[131] In short, rail regulation favored cheap goods at the expense of more expensive goods.

The ICC's approach to setting rates served farm interests (and rural interests) well, but value-of-service regulation, along with the more general cross-subsidies between high- and low-density lines outlined above, contributed to the steep decline in freight rail during the 20th century. During the 1930s, railroads carried roughly 75% of all intercity freight; by 1980, their share fell to 27% (see figure 1.11), while trucking increased. For example, between 1939 and 1967, the share carried by railroad dropped from roughly 62.4% to 41.6%, while the share carried by truck more than doubled, from 9.7% to 22.1%.[132] Rail regulation hastened these shifts. Value-of-service pricing and cross-subsidies work well when users have few alternative options—added costs can be built into prices and recovered. But throughout the middle decades of the 20th

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

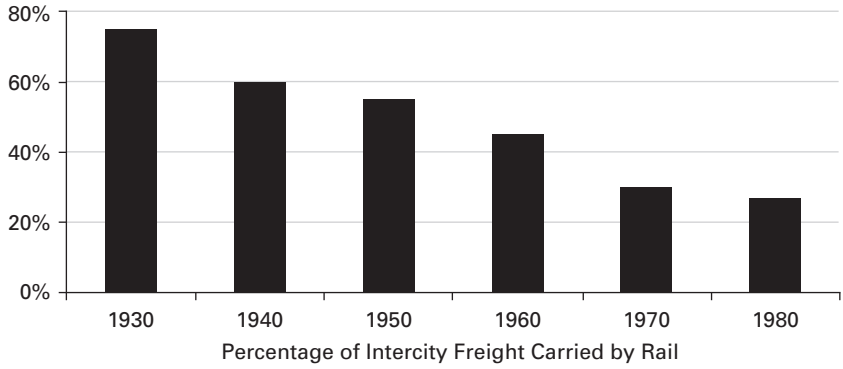


Figure 1.11
Percentage of intercity freight carried by rail, 1930–1980. Data from AAR, *Impact of the Staggers Rail Act*; Christensen Associates, *Description of the U.S. Freight Rail Industry*, 2-2.

century, trucks emerged as nimble competitors and provided shippers with the opportunity to opt out of the regulatory markup associated with rail regulation. Though the ICC regulated trucking under the Motor Carriers Act of 1935, the imposed regulatory burden for trucks was substantially less onerous when compared to rail. The ICC refused to lower rail rates to accommodate the development of new modes of transportation; it kept rail rates high even in the face of the steady erosion of market share. Additionally, the federal government provided support to trucking as it invested billions of dollars into creating the interstate highway system and improving roads during the 1950s and 1960s.[133] At the same time, a substantial portion of the trucking industry developed outside of ICC regulation. Trucks owned and operated by the shipper of the commodity—private hauling—were not subject to ICC regulation. Additionally, carriers of particular types of agricultural products were also exempt from ICC regulation. These efforts helped establish trucks as a viable alternative. It is unsurprising, then, to see the steady decline of freight traveling by rail and a growth in the share of intercity freight traveling by truck. Trucks captured portions of intercity freight that absent regulation would have been more cheaply handled by rail, such as long-distance travel. In short, regulation gave trucks an important edge and largely bound the hands of the railroads.[134]

The general picture of falling shares of intercity rail freight and increasing truck use was mirrored in the transportation of chemicals. Rail regulation inflated rates by roughly 20% for the shipment of chemicals, near the average for all commodities, and the markups above marginal cost

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

assigned to rail shipments of chemicals were double that of corresponding truck rates.[135] Though reliable figures are hard to come by, the Census Bureau's *Commodity Transportation Survey*, conducted as part of the larger economic census during 1963, 1967, 1972, and 1977, provides a snapshot of the shifting transportation patterns for industrial chemicals before deregulation. Between 1963 and 1977, the share of industrial chemicals transported by rail declined from 55.4% to 33.4%, while the portion carried by truck increased from 28.8% to 39%. These declines are in line with more general modal shifts (see figures 1.11 and 1.12).[136] There were, and are, stark differences in terms of how chemicals are moved via rail and truck. Typically, individual rail shipments move at roughly four times the size of truck shipments and travel greater distances between the point of origin and the destination.[137] Yet the structure of rail rates made it more attractive to producers and consumers to turn toward smaller shipments moving by truck.

Rail Regulation and Hazardous Materials

Regulation propped up an expansive, overbuilt rail network, and it encouraged patterns of transportation substitution—moving from shipment via rail to transportation via trucks—for particular commodities. As is discussed in the following chapter, this model of regulation would eventually bring the railroads to the brink of ruin during the 1970s. But these

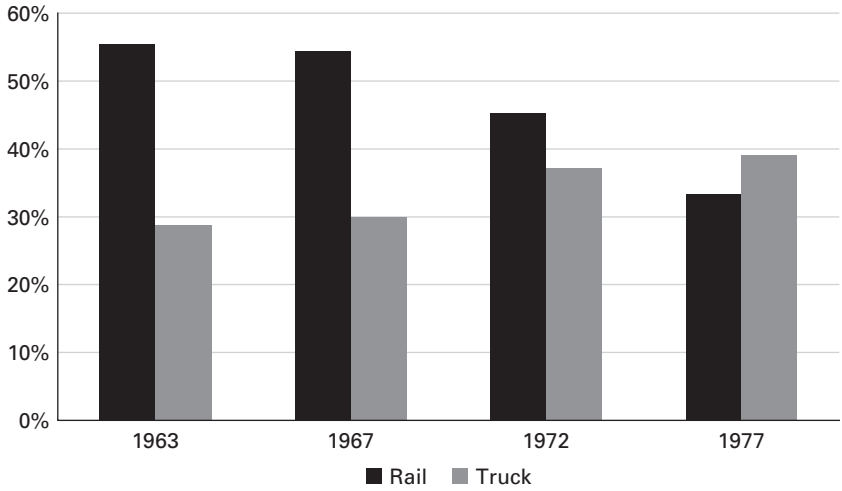


Figure 1.12
Percentage of industrial chemicals by mode of transportation, 1963–1977. Census Bureau, *Commodity Transportation Survey*.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

seeming inefficiencies were not without unexpected benefits. Regulation incidentally worked to combat normal accidents and provided a margin of safety that was easy to overlook. It did this in two main ways. First, the rate markup associated with rail regulation discouraged bulk shipments of chemicals via rail. The larger structure of rate regulation encouraged shippers to shift toward the use of trucks and, correspondingly, smaller shipments. Mixing large bulk shipments of chemicals and urban cities creates all sorts of possible unexpected interactions—interactions that can lead to tank punctures, derailments, and catastrophic accidents. Keeping large batches of hazardous materials off the rails reduces the risks associated with co-location and proximity—the risks associated with complexity that result when bulk chemical shipments travel through or near densely populated urban centers. Second, rail regulation supported an expansive and loosely coupled network. An expansive network with multiple shipping paths between any two points allows a degree of flexibility: trains can take circuitous paths, circumvent urban areas, or otherwise vary their routes. This allowed whatever residual shipments of dangerous chemicals were still traveling by rail to be potentially routed away from cities. Networks maximized for efficiency that are shorn of excess paths and contain only densely populated paths, on the other hand, are tightly coupled. There is little flexibility, and fewer opportunities to reroute hazardous materials. Carriers must travel the well-trodden path because it is the only path available. In these ways, regulation served as buffer against both complexity and tight coupling and lessoned the possibility of normal accidents.

Rail regulation encouraged smaller shipments of hazardous materials via truck, but what do we make of this trade? Trucks historically have a higher accident rate than rail. But the transportation of hazardous materials via rail *is* more dangerous (see chapter 2 and chapter 5). The transportation of hazardous materials in small batches by truck leads to more frequent but far less consequential accidents. Large bulk shipments via rail can lead to catastrophic impacts. Small shipments lead to accidents that have acute impacts; bulk shipments create possibilities for harm that can overwhelm a community. The risk associated with hazardous materials is tied to the property of the carried material, the amount of material present, the exposed population, and the likelihood of an accident.[138] The transportation of massive shipments of hazardous materials via railcars near urban areas creates the possibility of a catastrophic accident—a rare but exceedingly damaging event. The structure of rail rates pushed the transportation of chemicals toward smaller batches of materials and shifted the risk away from a catastrophic event, toward a

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

series of localized and more manageable failures. Small, comparably frequent accidents involving trucks carrying hazardous materials are, to be clear, not welcome. But the possibilities of harm associated with bulk rail shipments are different. Tens of thousands of casualties could result from an accident or attack targeting bulk rail shipments (see chapter 2). This sort of hazard—the possibility of harm on a scale difficult to imagine and difficult to address through emergency response—would become central to post-9/11 infrastructure management.

Like the post office, the particularities of regulation were encoded within the day-to-day structure and operation of the material network. Key features of the system—where track sat, the path that railcars took, and the mix of commodities that railroads carried—were shaped directly and indirectly by regulation. Looking back through the prism of later post-9/11 debates and anxieties over the safety and security of shipments of hazardous materials, rail regulation provided some overlooked benefits. It discouraged the bulk transportation of hazardous materials in favor of smaller shipments. And it kept alive an expansive rail network that made it (at least theoretically) possible for residual shipments of dangerous cargo to avoid densely populated urban centers. These were real, if at the time unintended and unacknowledged, benefits. Keeping large quantitates of hazardous materials physically separate from urban areas makes good sense: it reduces the unexpected interactions that can occur between dangerous materials and the day-to-day life of the city. Normal accident theory offers a simple point: colocation of dangerous technologies and other complex systems (a city qualifies) creates a recipe for disaster. Or, to put it another way: lots can go wrong when a railcar carrying 90 tons of chlorine moves through a city.

A Network of Networks: Electric Power, Regulation, and Control

In the postal system and freight rail network, regulatory practice was centered within the federal government. In electric power a mix of state and federal regulations worked hand in hand. Regulation promoted a loosely coupled network of vertically organized local monopoly providers. It organized the electric power system into a "network of networks," to steal the oft-used description of the Internet. Power was produced and consumed within circumscribed regions, and control was distributed throughout a network of (mostly) investor-owned utilities (IOUs). Each system was autonomous while interconnections with adjacent systems provided an added backstop in case of localized outages and failures. IOUs

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

took charge of the three phases of electric power—generation, transmission, and distribution—for a limited geographic area and coordinated these operations through internal, rather than interfirm, systems of control. Regulation countered efforts to tightly couple these systems, leaving them loosely joined. This model offered real benefits: failures were mainly isolated within an individual system.

Regulation did not only shape the outline of electric power systems; it also shaped their guts. It molded how electric power companies would employ new technologies *internally*. While debates about how best to organize the industry unfolded in Congress, boardrooms, and statehouses across the country, engineers working within the industry grappled with recurring challenges related to the control of the material network. An enormous amount of informational work was needed to coordinate and control electric power systems; as these systems became connected at the edges, these challenges became more complicated. The broader regulatory structure—political and economic controls over the industry—shaped these informational practices by supporting the development of and investment in new devices and technology. The specific structure of utility regulation encouraged IOUs to invest heavily in new information and communication technologies (ICTs) and supported the industry's early adoption of analog and digital computers. Rate-of-return regulation supported a particular model of computing—control systems that were idiosyncratic and linear. These systems were difficult to access or alter because they were not generative machines or systems that could be easily accessed and reprogrammed for different purposes. They were produced and designed for specific tasks. This model of computing—which, to be clear, dominated computing for much of the middle decades of the 20th century across all industries—made it difficult for outsiders to manipulate or subvert the computerized control systems and networks that increasingly became central to electric power.

State Regulation of Electric Power

The regulation of electric power, like that of the railroads, did not emerge over the opposition of private industry. It found vocal and important champions from within industry. Pioneering entrepreneurs in the business of electricity promoted the notion of natural monopoly—that electric power was best operated by a single provider—and solicited state regulation as a way of increasing productivity and market power and deflecting the surging challenge from municipally owned and operated power providers.[139] Progressive civic groups and reform governors joined with industry advocates in arguing for the necessity and virtue of state regulation.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

For reformers, state regulation offered a way to combat the endemic local corruption attached to municipal control. The ultimate success of the state regulation of private monopolies was largely due to the intersection of the efforts of both industry and reformers: political maneuvering, less than technological inevitability, accounted for the institutionalization of the form.[140] Between 1907 and 1922, 32 states created state regulatory commissions to oversee the operation of private monopolies, and the basic structure of the industry was set firmly in place.[141]

This outcome was anything but a foregone conclusion. In the decades following Thomas Edison's launch of the Pearl Street Station in New York City in 1882, different approaches to organizing the provision of electricity jostled for supremacy. In addition to the well-documented battle of the currents between Edison's direct current (DC) and Westinghouse's alternating current (AC) systems, different schemes for providing power—including local competition between multiple private firms, municipally owned and operated systems, on-site "isolated" systems, and cogeneration—flourished.[142] The eventual institutionalization of private vertical monopolies owed much of its success to the efforts of Samuel Insull. Insull served as Thomas Edison's secretary from 1881 to 1892 before taking over as the head of the then small Chicago Edison Company. He would become one of the most powerful businesspeople in America. He went on to dominate electric power during the early 20th century (and other areas of commerce). At the peak of his success, Insull was worth more than $100 million and controlled thousands of utilities through his holding companies. He operated in over 30 states, and his businesses served 6.3 million people.[143] Insull was a towering figure, deeply involved in both politics and cultural life. Orson Welles based *Citizen Kane* in part on him as well as William Randolph Hearst.[144] Insull's success and great innovation lay in recognizing and then successfully realizing the opportunities afforded by monopoly service and new forms of steam generation.[145] He promoted *centralized systems*, large generation units linked to a set of customers through a transmission and distribution network.[146] In retrospect, his approach seems deceptively simple. Electric power cannot be readily stored. Generation and consumption must occur simultaneously, and demand varies greatly depending on the time of day and type of customer. Residential consumers during the early 20th century, for example, used electric power mainly for lighting and, as a result, demand for power would spike in the evening hours after work and decrease during the day. To meet demand, utilities would have to invest in generating enough capacity to meet peak load (demand), which would sit dormant during

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

nonpeak hours. Insull recognized that capturing demand diversity was essential to realizing economies of scale and maximizing the return on investment in large steam turbines. Rather than catering to a homogenous market in which demand varied in lockstep, Insull sought a mix of different customers with complementary demand curves (patterns of use) so that demand would be spread somewhat evenly.[147] To take a basic example, by catering to both industrial consumers, whose demand spiked during the day, and residential users, whose demand peaked at night, the electric system could be more effectively utilized and greater returns earned.[148]

Insull faced a stiff challenge. Competition frustrated attempts to build a diverse portfolio of customers. Potential industrial customers cheaply produced their own power on-site, a form of cogeneration, as a by-product of industrial processes, while isolated plants, such as on-site home and business generation systems, were widely used.[149] In other cases, cities offered franchises to multiple competitive private providers or operated their own municipal power systems.[150] Municipal systems, however, presented the greatest challenge to the viability of private power systems. Between 1895 and 1906, public systems grew at twice the rate of private systems and accounted for 30% of the nation's electrical suppliers, as cities turned toward public ownership as an alternative to private operation.[151]

Insull attempted to subvert these forms of competition. He offered industrial customers and consumers drawing power at nonpeak hours deep discounts, effectively siphoning off the most prized customers, and he aggressively pursued the acquisition of rivals to limit local competition.[152] But these strategies, ultimately, were limited. Insull turned toward state regulation as a way of checking the growing swell in favor of municipal power and limiting the availability of alternate suppliers of power. Insull became a powerful proponent of state regulation and pushed the larger power industry to follow his lead. Regulation, he hoped, would snuff out competing ways of organizing electric power and help institutionalize private vertical monopolies.[153]

Insull and his associates promoted state regulation through the two most powerful industry trade associations—the Association of Edison Illuminating Companies (AEIC) and the National Electric Light Association (NELA)—and the National Civic Federation (NCF), a national Progressive organization where he served on the executive committee.[154] Insull advanced the idea of regulation as a useful alternative to municipal power in a speech before the NELA as early as 1898. It was initially received with horror. Members of industry rejected the notion of regulation almost as an article of faith. Gradually, over the next several years,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

as Insull's associates rose to dominate industry trade groups, the industry came to embrace his views.[155] Once they embraced state regulation, utilities found powerful allies in public reformers and the Progressive movement. Governors Robert La Follette, Charles Evans Hughes, Hiram Johnson, and Woodrow Wilson, despite their many differences, viewed municipal power as bastions of local corruption. They saw state commissions as important remedies that could act as fair dealers and provide franchises in an uncompromised manner.[156] Progressives, too, accepted the basic public position of the industry—that electric power was a natural monopoly—and saw state regulation as a means of harnessing the benefits of electricity for the public good.[157] State regulation emerged from this confluence of interests, joining businesspeople and reformers. In 1907 the NCF promoted Insull's position and drafted model legislation chartering state commissions; Wisconsin, New York, and Massachusetts adopted regulatory laws creating state commissions based on the NCF's model legislation during the year (the Wisconsin law was directly taken from the drafted text). Other states quickly followed their lead, and state commissions became standard.[158]

The Outline of State Regulation

State commissions provided the basic regulatory mechanism that institutionalized Insull's model of power. Under this model, private utility companies yoked together generation, transmission, and distribution. State public utility commissions, in broad strokes, controlled entry through the granting of exclusive franchises for power companies to operate within a finite geographic territory and controlled rates through rate-of-return regulation.[159] Regulation foreclosed alternate possibilities and pathways: the birth of state regulatory commissions effectively sucked the air out of the municipal power movement and explicitly supported vertically organized systems at the expense of different models such as cogeneration, on-site power, and competitive provision.[160] State regulation deflected the challenge of municipal ownership by legitimating private ownership and addressing, to a degree, complaints about private ownership and operation. The total number of municipal power systems peaked in 1922, with 2,500 utilities providing 5% of the nation's generating capacity.[161] The model that became common—vertically organized private monopolies—was not, to be clear, necessarily the most efficient: cogeneration, on-site systems, and municipal ownerships all had their merits, and a clear, unequivocal, technical case against them cannot be made. But state regulation created new barriers to alternate forms of power production and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

generation while providing private vertical power systems with generous benefits.[162]

As in other industries, regulation operated as a quid pro quo that provided both private capital and the public with benefits. Licensed companies, most importantly, were protected from competition, and state commissions set rates that provided a stable, guaranteed return on investment through what is known as *rate-of-return regulation*. Power companies were now easily able to aggregate diverse sets of users and attract outside investment, a necessity due to the high fixed costs associated with electric power systems and a notoriously difficult achievement under the previous conditions of hit-and-run competition and possible municipal takeover.[163] Regulation also enabled private companies to use eminent domain in siting power plants, lines, and other facilities. The public also reaped substantial rewards from the regulatory compact. In concert with exclusive franchise, power companies were essentially treated as common carriers, obligated to build out systems to serve all customers at fair, nondiscriminatory rates and provide reliable service.[164]

Toward Super Power? Federal Regulation and the Preservation of Loose Coupling

Federal regulation intervened at a critical moment in the development of electric power. It checked the consolidation of scattered local systems into centralized regional systems or even a national power system. During the interwar years, competing public and private movements sought to transform the organization of electric power and exploit the new possibilities of interconnection that the war effort revealed. These movements sought to replace the loosely interconnected network of networks—interconnected autonomous vertical monopolies that Thomas P. Hughes describes as something akin to a "confederation of nation-states"—with a single system under central control covering vast regions or the entire nation.[165] Ultimately, the Public Utility Holding Company (PUHCA) Act of 1935 provided a break on these competing moves toward consolidation and maintained the independent and loosely coupled architecture of electric power as it had previously existed.

World War I: Creating an Interconnected Network

Before World War I, most electric power systems lacked interconnection; power systems were not linked to one another but rather were configured as isolated networks operated by a single utility.[166] During World War I, however, adjacent power companies began to enter into power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

pools in order to share power to meet the growing demand driven by the war effort.[167] Wartime mobilization created spikes in demand and a new urgency for access to power. To this end, the War Industries Board, along with state and federal authorities, encouraged and in some cases, directly ordered, interconnection.[168] The interconnection of adjoining systems through new high-voltage transmission lines offered a way of maximizing capacity with little investment and without the long lead times of creating new power plants.[169] In some ways, the drive toward continual integration of systems was the logical conclusion of Insull's model. Improvements in high-voltage transmission lines during the first decades of the 1900s steadily increased carrying capacity and made interconnections possible.[170] Through interconnection, surplus power could be used between systems: as one system approached peak capacity, the excess power of an interconnected, underutilized system could be brought online as a supplement. Just as interconnecting different customers within a city proved a boon for electric power companies, interconnections between systems served to increase load factor by matching diverse demand portfolios across broader regions. Interconnection not only provided an economical way of supplying backup power during periods of peak demand but also offered a reserve in case of unexpected outages: if a generator failed or a component of the system stopped working, power could be solicited and drawn from an interconnected system to satisfy demand.[171] Importantly, systems participating in power pools and interconnections, however, remained independent and loosely coupled—recall how during the blackout of 1977 interconnected electric companies were able to splinter from Con Ed with little interruption. As historian of electric power Julie A. Cohen notes, interconnection initially provided both "unity and autonomy."[172] Individual electric power systems controlled the flow of power through their individual network and remained autonomous.

Super Power, Giant Power, and the Holding Companies

Wartime interconnection proved the viability, and in some cases the desirability, of connecting previously separate systems. After the war, throughout the 1920s and early 1930s, numerous public and private schemes attempted to follow this trend to its logical conclusion and push toward consolidating loosely conjoined local networks into a set of vast regional systems or even a single national power system. From within government, the Department of the Interior and the governor of Pennsylvania championed creating the foundations for a consolidated regional or national power system under projects that would, in effect, replace local power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

systems with a centralized public power system. At the same time, the consolidation of ownership within electric power through the use of highly leveraged holding companies sought to effect the same basic transformation, although, importantly, with the caveat of substituting the dominance of private industry in place of possible public control and oversight. These interwar movements and countermovements were a contest over who would control the newly reorganized power network—whether the state or private capital would dominate the (seeming) future of electric power.

During the 1920s, the Department of the Interior and, later, Commerce Secretary Herbert Hoover, along with the governor of Pennsylvania, Gifford Pinchot, advanced public plans to reorganize and consolidate electric power under public direction as a way of rationalizing electric power and extending service to rural communities while avoiding the pernicious influence of private capital through the growing *power trusts*.[173] These plans, known as *Super Power* (or Superpower) and *Giant Power*, respectively, differed in their specifics, but both advanced aggregating the scattered sets of individual power systems into larger regional entities or even a single national system under the central direction of a new governmental entity.[174] The plans received broad coverage in the press but faced bitter opposition from the utility industry.[175] Industry attacked both projects, even the more modest Super Power plan championed by Hoover, a strong supporter of private utilities, and charged that the public plans touting state and federal supervision of new interconnected systems were "communistic." They worked to block the advancement of the plans.[176]

At the same time that Super Power and Giant Power were under evaluation, private industry undertook its own program of interconnection and consolidation outside of direct state stewardship. Beginning in earnest during the 1920s, highly leveraged holding companies consolidated ownership of multiple power systems. Holding companies operated in a pyramid fashion, stacking subholding companies that did little but hold securities in the companies below. These companies allowed the holders of stock at the top of the pyramid to control a bundle of operating companies with little investment through the division of issuances of common and preferred stock. Samuel Insull was a key player. At one point, he controlled companies serving 5,300 communities in 32 states with assets above $500 million with only $27 million in investment.[177] Though holding companies had been involved with utility companies since the early days of electricity, it was not until after World War I that they began to dominate the industry.[178] In addition to fostering leveraged structures, holding companies also notoriously overvalued assets and padded expenses as a

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

way of circumventing state regulations on profits. This gambit provided handsome returns for those who controlled stock at the upper levels of the pyramid.[179] The holding company movement reached its peak during the early 1930s, when 16 holding companies controlled 90% of all the electricity in the U.S.[180] This change in political economy produced an echo in the structure of the physical networks, as operational integration followed economic consolidation. Transformations of the ownership and control over IOUs fed the growth toward increasingly centralized electric power systems. Holding companies sought to effect the changes outlined in the proposed Super Power and Giant Power programs—consolidation and integration of scattered geographic networks into a single operating unit, knitted together with high-voltage transmission lines fed by large generation facilities—though, of course, under the auspices of private authority instead of public supervision. As holding companies swallowed up previously independent operators, independent systems were then transformed into larger units under centralized control and operated as one network.[181] For example, the United Corporation, chartered in 1929 by J. P Morgan & Co. in partnership with two other investment houses, controlled five major holding companies and, by extension, numerous utilities across the Northeast and Southeast. Through such financial arrangements, J. P Morgan in effect controlled more than one-third of the nation's electric supply.[182] After incorporation, holding companies began the process of interconnecting their utilities across the East Coast into a system that looked much like the proposed Super Power system, and rumors of a possible national monopoly under private control flourished.[183]

During the 1920s and 1930s, reformers and the industry struggled to define who would control the reorganized system of electric power. Both movements took for granted the inevitability and desirability of merging formerly distinct networks into larger systems but differed as to the terms on which such a change should unfold. Pinchot saw his model of public intervention as an explicit reaction to and rejection of the growth of holding companies and private power. For him, the growing empires of electricity presided over by holding companies mimicked "an enchanted evil spider … hastening to spread his web over the whole of the United States" and presented a clear choice: "Either we must control electric power … or its masters and owners will control us."[184] These movements attempted to nudge electric power systems toward a tightly coupled architecture; geographically bound independent systems began to give way to increasingly larger regional operations with control—and, as a result, risk and vulnerability—aggregated at correspondingly higher levels.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Federal Regulation: The Public Utility Holding Company Act of 1935

Federal legislation blocked these competing movements and preserved the loosely coupled network-of-network structure of electric power systems. The Public Utility Holding Company Act (PUHCA) of 1935 rolled back the clock, as it were, and pushed back against the drive toward consolidating systems into larger aggregations. The act was a conservative resolution to the competing public and private movements toward consolidation. While private utilities parried and defeated Super Power and Giant Power, holding companies were not left untouched. The PUHCA, like other pieces of New Deal legislation, struck a balance between preserving private capital and limiting the more deleterious effects of private power. It extended and reinforced public accountability over electric power but, as with other infrastructures, it did so through compromise and quid pro quo.

Public dissatisfaction against the power-holding companies had been growing since the mid-1920s. At the behest of Congress, the Federal Trade Commission (FTC) began a high-profile public investigation into the holding company issue in 1928. The FTC's 6-year study uncovered and publicized a myriad of financial irregularities and abuses at the hands of holding companies.[185] The Great Depression hit holding companies, and their leveraged structure, particularly hard and forced many into bankruptcy, ruining scores of investors in the process.[186] Insull, a symbol of corporate power and a key architect of the growth of electric power, was ruined—forced out of his companies, bankrupted, and later put on trial for fraud.[187] His investors lost a fortune. As John F. Wasik notes in his biography of Insull, these investors, which included truck drivers, plant foremen, meter readers, and others, lost in total $750 million during the crash, equivalent to roughly $13.5 billion in 2017.[188] Franklin D. Roosevelt capitalized on the rising outrage over holding companies, then seen as symbols of financial avarice that had helped capsize the economy, and targeted the power trusts' control over electricity as a central part of his campaign platform in 1932. Roosevelt made his ire known, stating that holding companies were "a corporate invention which gave a few corporate insiders unwarranted and intolerable powers" and that he stood against the "Ishmaels and the Insulls, whose hand is against everyman's."[189]

As part of the New Deal, FDR moved to implement federal legislation to break up holding companies.[190] State commissions were unable to exert real regulatory oversight over the holding-company empires, as their ownership of multiple franchises in different states amounted to interstate commerce and, as a result, placed them beyond the effective ambit of state authorities.[191] The PUHCA of 1935 attempted to reform

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the utility industry and return regulatory power to the states. The act enabled the Securities and Exchange Commission (SEC) to oversee dividends, loans, security issuances, and property transfers; approve new acquisitions, and impose uniform accounting provisions on utility companies.[192] The central provision of the act, section 11(b), the so-called death sentence, attempted a more thorough reform of utility operation. Section 11(b) called for the breakup of interstate holding companies into various single, geographically contiguous operating companies. The vast empires under holding-company control, made up of scattered utilities operating across states, were no longer tolerated. Now, companies could only operate a single "integrated system" that served a limited area.[193] Section 11(b) sought to limit the ongoing accumulation and unification of scattered regional systems by holding companies and, rather, bracket the operation of utilities to a single system that could, now, be effectively regulated under the jurisdiction of a state regulatory commission. The PUHCA, in effect, returned power to the states.

The act did not mandate the abolishment of all holding companies and made allowances for the retention of small, otherwise uneconomical systems.[194] Yet the intent and eventual implementation of the act was to attack the growing "bigness" of utility systems and the consolidation of power behind holding companies and to support local—that is, state—control of limited systems.[195] The SEC broadly interpreted the act and held that the breadth of a system alone, the size of a system, could provide adequate grounds for ordering divestment.[196] The act reversed the trajectory of the holding companies toward the greater integration of scattered systems and led to hundreds of systems separating back into independent entities.[197] Between 1935 and 1950, the number of holding companies registered with the SEC dropped to fewer than 20 while over 750 systems with assets valued at over $7 billion were divested from various holding companies.[198] The PUHCA, along with state regulation, preserved and supported a patchwork network of vertical monopolies serving limited areas. The drive toward tight coupling, for a time, receded in the face of new regulatory provisions.

Regulation and Control: Political Economy and Information and Communication Technologies

By 1935 the outlines of public control over electric power were sliding into place: state public utility commissions oversaw vertical monopolies, and federal law and regulation served as a backstop that limited the consolidation of systems and ensured that utilities did not outgrow the supervision of state commissions. Private companies operating territorial monopolies

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

were connected at the edges; they could and did provide power to one another during emergencies. But this interconnected system preserved the autonomy of the individual utilities—each utility controlled its own system. Each coordinated its system through internal control networks and related informational work. This model was loosely coupled, and each system stood, more or less, on its own. If one steps back to survey the state of electric power, what appears is not a single network but rather a collection of autonomous, centrally managed, territorial monopolies.[199]

While debates about the proper role of public and private companies unfolded during the late 19th and early 20th centuries, a related debate played out among engineers and equipment manufacturers.[200] They confronted increasingly complicated control challenges through debates in journals, conferences, and meetings of industry associations. A great deal of informational work went into maintaining electric power systems. These systems must constantly balance load (demand) and generation (supply). Disjunction of supply and demand—generation above or below demand due to unplanned component failures or unforeseen swings in supply or demand—can lead to failure.[201] Additionally, all interconnected power generators must operate with the same frequency. As load changes, generators can speed up or slow down, and the system can fall apart.[202] The different components of the system must operate in close coordination. Control challenges multiplied as electric power systems continued to grow in size and were increasingly interconnected with one another. The broader regulatory structure of the industry influenced how these control and coordination challenges would be solved: it supported significant investment in new information and communication technologies (ICTs), including analog and digital computers, that could aid the informational work required. Here, as in the case of the postal system, the regulatory model made an impact on the material technologies used for system control. Where postal regulation continually supported the use of manual techniques for processing mail, the regulation of electric power supported the early investment and adoption of new computing technologies. Rate-of-return regulation encouraged and rewarded investment—even overinvestment—in new capital. As a result, electric power utilities invested heavily in the development and acquisition of ICTs customized to their particular needs. These new ICTs replaced or augmented long-standing information practices, but they maintained a linear mode of control: these ICTs were designed for and dedicated to a narrow range of specific tasks.

During the 1920s and 1930s, engineers and researchers were preoccupied with the problem of network stability. Interconnection with neighboring

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

utilities and the continuous growth of utility systems presented ongoing control challenges. To confront these challenges, each utility's load dispatcher and dispatching center performed close monitoring and control over their system. They used an evolving mix of tools to both forecast expected demand and measure current system performance. A central task for electric power operators was estimating fluctuations in demand. Demand fluctuates due to predictable variables, in accordance with time of day, seasonal variation, and other well-anticipated changes that routinely influence power consumption, as well as unforeseeable short-term issues, such as atypical weather or operator error. From the earliest days, utilities created detailed tables and statistical measurements—informational work—of historic trends of demand and capacity in order to estimate required loads. Early telemetry systems provided system operators with readings about output, load, and the status of generating units and switches in the network.[203] Dispatchers were linked to remote portions of the system through dedicated telegraph and telephone lines and, later, carrier communications over power delivery facilities and microwave channels. Later advances in control allowed them to manipulate the system in real time. These methods of control allowed the electric power systems to be closely managed.

The development of techniques of control did not occur outside of the larger political economy of electric power. Rate-of-return regulation supported the development and eventual deployment of increasingly specialized ICTs for power system operations. Under rate-of-return regulation, R&D and capital costs were included in calculating the rate base upon which utilities were guaranteed a certain percentage return, while labor and fuel costs were not included in the rate base and were directly passed on to the consumer.[204] Regulation, as a blunt instrument, created a system of incentives that encouraged utilities to seek out and invest heavily in new, costly capital projects and research (though they often bypassed research in favor of capital), regardless of the cost savings or efficiency gains. Under rate-of-return regulation, firms could invest in capital-intensive projects and technologies as a way to expand the rate base and, consequently, increase profits.[205] Historically, state regulatory commissions rarely challenged or disallowed utilities from including particular capital costs in the calculation of the rate base nor were they quick to lower rates if new cost savings materialized.[206] Under this model the electric utility industry became the largest industry in the U.S. in terms of gross capital assets.[207] Unlike the postal system, where regulation supported labor over technology, the regulation of electric power encouraged investment in

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

technologies above all else.[208] Key beneficiaries and supporters of rate-of-return regulation were the equipment manufacturers that supplied industry: General Electric (GE), Westinghouse, and Leeds & Northrop, most obviously.[209] In this light it is unsurprising to find that utilities were quick to invest in and adopt new, expensive technological solutions to problems of control.[210]

Initially, calculating equipment and computers offered utilities a way to study the stability of large power systems through models and assisted in solving complex differential equations.[211] During the early 1920s and early 1930s, GE was a key source of support for the work of Vannevar Bush and his colleagues at the Massachusetts Institute of Technology (MIT) Electrical Engineering Department.[212] Their work on the impact of transients—short-term, passing phenomena such as lightning strikes, increases or decreases in load or generation, and short circuits—on system stability led to the development of two early analog computers: the network analyzer and the differential analyzer. The network analyzer served as a programmable scale model for electrical systems that could be used to simulate power system behavior. The differential analyzer simplified the work of computing complex differential equations associated with the analysis of power system operation.[213] MIT offered both devices for use to commercial clients, such as GE, American Gas and Electrical Services, and other utilities; these devices were later reproduced by GE and other universities.[214] GE's main competitors in the electric equipment market, Westinghouse and Leeds & Northrup, developed their own computational equipment as well. After World War I, Westinghouse built DC and AC calculating boards that could approximate network behavior and during the 1940s, in partnership with the California Institute of Technology, built the analog computer Anacom to study system stability.[215] The differential analyzer, in particular, was used in developing ENIAC, one of the first digital computers.[216]

During the 1950s, electric power companies began to adopt computers directly into their day-to-day operations for system management, rather than as tools that only provided modeling and off-line analysis of system stability (see figure 1.13). Utilities integrated off-line and real-time computer systems into their operations to aid system stability, economic dispatch, demand forecasting, contingency planning, and other functions. Leeds & Northrup, IBM, GE, Westinghouse, and other suppliers provided equipment and systems utilizing computers for utilities during the 1950s and 1960s. One of the early computer systems designed for power systems, Leeds & Northrup's Early Bird, was available in 1954 and subsequently adopted by a host of utilities at a steep price of between

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

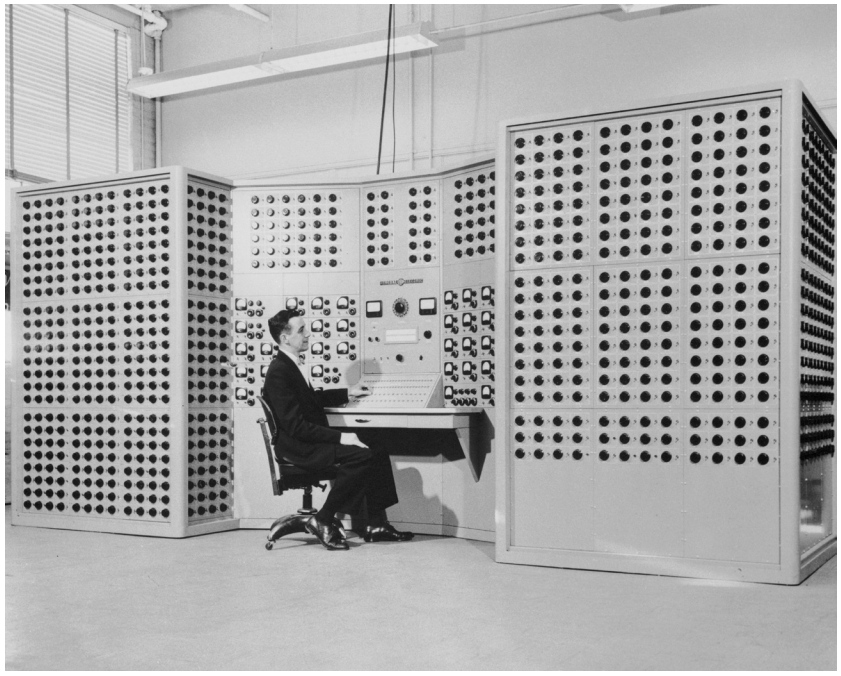


Figure 1.13
General Electric computer engineering supervisor K. R. Geiser tests a dial-studded computer to model the electric power system, 1955. The computer's 1,290 dials are set to simulate physical facilities and load conditions within a 46,000 mi.^{2} service area. The computer would go into service at the Nerve Center of the American Gas and Electric System in Columbus, Ohio. Image courtesy of Getty Images. Caption edited from the original.

$50,000 to $150,000 per unit.[217] In 1961, Louisiana Power and Light opened what was considered to be the first fully automated power plant, its Little Gypsy station outside of New Orleans, with equipment designed by Daystrom. Through the 1960s, power plants adopted analog and digital computer systems to control operations with equipment from a variety of suppliers.[218] These systems supplemented, or in some cases replaced, the direct wire and basic telemetry systems then in use. They were designed under contract for specific facilities and were not offered as one-size-fits-all, commercial off-the-shelf products. These systems mixed computation and control. They automated some of the work of system operations and provided operators with better control and information about the system. New computer-based control systems were used to preserve system stability. One of the functions of newly installed computer systems was to match supply (load) and demand (generation). These systems assisted with load

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

balancing in a number of ways: they monitored system performance and made corresponding adjustments to meet fluctuations, through what is known as automatic generation control (AGC); they archived historical data on system performance to create detailed forecasts that helped guide the adjustment of generators; and they performed contingency analyses to alert operators to possible critical system failures.[219] New computer systems were also used to execute economic dispatch—a process for determining the optimal and cheapest combination of the multiple available generators connected to the power system. Computer systems compared the total required load against the incremental cost for the generating assets based on fuel costs, unit costs, and transmission loss and performed dispatch to meet the total power need at the lowest total cost.[220]

In many ways these computer systems were typical for the period. They were expensive and massive installations. The Little Gypsy power station used two Daystrom 046 computers.[221] Each of these machines weighed 9,000 lbs. and spanned 9 ft.^{3} of floor space.[222] They were specially designed for a utility. Once contracted, it took Daystrom a year to produce a machine.[223] Importantly, these machines were customized and dedicated to a fairly specific range of tasks. Despite the technological advances that computerization represented, these machines were still, at their core, linear technologies. Their functionality was locked down and narrow. Reprogramming or altering these computer systems—adding new functions—was not simple. This model of computing—dedicated systems that were difficult to alter—would later be replaced by generative systems, accessible multipurpose machines that could support different sorts of programs and that could be altered with little difficulty (see chapter 2).[224] Generative systems are rightly celebrated for their ability to support innovation and unanticipated discovery.[225] But the older model of computing, in retrospect, had significant benefits as well. These types of dedicated systems were linear and programmed to be task-specific. Because altering them was difficult, they were both inflexible and difficult to adapt to new tasks. This inflexibility made these machines difficult to hack or subvert. They could not be easily repurposed for malicious (or benign) purposes. Control systems were hard to access—rarely did they operate on open and accessible public networks—and reprogramming them to operate in different ways was not easy or always even possible. These systems were engineered and designed not as general computing platforms that could support and run different types of programs; they were built by suppliers for specific tasks on contract. This approach was costly, but it fit well with the regulated paradigm: investing heavily in

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

equipment was strongly encouraged. Decades later, as fears over "hacking the power grid" became prevalent (see chapter 2 and chapter 6), the overlooked and unintended virtues of this older model of computing would move into focus.

The Regulation of Power and the Power of Regulation

State and federal regulation maintained a loosely coupled network of interconnected electric power systems. Under the legal framework created during the early decades of the 20th century, state regulatory commissions oversaw franchises operating autonomous vertical monopolies, while federal regulation, through the PUHCA and the auspices of the SEC, checked the growth and consolidation of these systems into larger configurations. The structure of state and federal regulation maintained a patchwork confederation of systems, a network of networks interconnected for reliability and support but functionally distinct. In this manner, regulation supported loose coupling: each system maintained hierarchical control over its own network and oversaw the coordination of generation, transmission, and distribution. In doing so, regulation provided a hedge against large-scale failure and systemic vulnerability. Distributed control prevented the aggregation or accumulation of risk; failures of any single utility system were limited to the scale of its operating territory. Though vertical monopolies were linked to larger regional grids, these linkages were designed so they provided access to additional resources without the cession of control.

At the same time, rate-of-return regulation supported the development and adoption of new ICTs. Regulation shaped how new ICTs were incorporated into the provision of electric power. The broader political economy of electric power shaped how utilities confronted recurring challenges of control. Namely, it encouraged the adoption of new and expensive ICTs dedicated to well-defined tasks—linear technologies. In doing so, it limited the degree of complexity found within electric power. The later adoption of multipurpose and standard commercial equipment would create significant new challenges for electric power. The overlooked security benefits of this older model of computing would only become clear in retrospect.

Stumbling toward Resilience: Revisiting and Rethinking Infrastructure Regulation

Reexamining the history of infrastructure regulation through the lens of normal accident theory reveals a largely overlooked virtue: resilience. The historical experience of regulation helped push these systems into

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

particular configurations. Infrastructures did not develop outside of or in opposition to the political arena. Rather, they were deeply entangled with regulatory policy and practice. The particularities of regulation became embedded within the very structure and operation of these systems. Regulation operated differently in each sector and, consequently, left different imprints on each system. The structure of regulation in the postal system, for example, starved the Post Office Department of capital for technical improvements. It supported distributed processing and a reliance on labor over new and costly technologies. In electric power, however, regulation operated quite differently. It offered generous support for investment in new technologies while also preventing the growth of large consolidated systems. This makes it difficult to offer sweeping statements about the relationship between regulatory oversight and technological development; in some cases, regulation supported heavy investment in new technologies and in others it did not. Yet in each case examined, regulation fed resilient configurations.

Regulation, at bottom, sought to make infrastructures publicly accountable. Resilience, when it appeared, was an unintended side effect. The power of the state served to counterbalance the power of infrastructure operators and certain customers. It made sure that these systems did not *only* serve the ends that the market would support; it made sure that, however imperfectly, different infrastructure publics were acknowledged and served. It often did so in a conservative manner—enacting a quid pro quo that gave real benefits to incumbents and powerful players (Insull and other private electric power companies did not seek state regulation out of the goodness of their hearts) while also securing tangible benefits for other infrastructure publics. Regulation imposed common-carrier obligations, helped build out and make infrastructure services widely available, and restrained the baldest abuses of power. Regulation provided concerned parties a venue to voice their concerns and have a hearing; it provided a way of reconciling the repeated disputes between various infrastructure publics. It explicitly attested to the fact that these systems were more than simply another type of business—they were, as *Munn v. Illinois* argued, imbued with a larger public interest.[226]

This system of regulatory control, incidentally or accidentally, built into these systems a degree of resilience. To be sure, at times these configurations were not the most efficient possible. Yet entwined with these inefficiencies were benefits that were easy to overlook and ignore. Support for resilience was not an intended consequence of regulation. Rather, regulatory practices stumbled into resilience as they sought to accommodate other goals and sets of competing interests. Regulation supported loose

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

coupling and linearity and at times actively blocked the push toward tight coupling and increasing complexity. In doing so, it helped create and maintain systems that could cope with localized failures. In the postal system, regulation ensured that the network was loosely coupled and redundant. Processing—control—was distributed across the network. In individual post offices scattered across the nation, armies of clerks processed, and continually reprocessed, mail based on memorized routing schemes. Each post office was vital to its local community and integrated into a national network, but the failure of any particular office did not threaten to capsize the larger integrated network. The structure of the network ensured that local outages were minor disruptions, rather than systemic failures. Put another way, local failures remained just that—local failures. The ICC's oversight of the nation's freight rail system had unexpected benefits as well: it served as a de facto tax on the transportation of dangerous materials, and it undergirded a rail network that allowed residual shipments of hazardous materials to potentially travel on routes that avoided cities. Accidents involving hazardous shipments, of course, were not eliminated, but the risks were reduced. In electric power, regulation created limited territorial monopolies and supported the adoption of dedicated ICTs. This did not prevent blackouts, but it did ensure that, in most cases, a local blackout would not spill over to other neighboring systems. Likewise, the adoption of dedicated ICTs did not make the malicious manipulation of ICTs impossible—but it did make it more difficult. These various systems were not, to be certain, free from their share of disruptions or failures. However, the architecture of the systems helped to ensure that such failures were limited in scope and scale.

Yet while politics could undergird resilient systems, they could also, in a quick breath, turn to undermine them. Beginning in the 1970s, deregulation remade how infrastructures operated. The drive to capture new efficiencies undermined long-standing public checks on infrastructure and, in the process, subverted these historic supports for resilience. While the restructuring of infrastructures delivered new efficiencies, it would do so at a price.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

2

The Political Origins of Infrastructure Vulnerability: The Hidden Vices of Deregulation

Our present postal system is obsolete; it has broken down; it is not what it ought to be for a nation of 200 million people.… And now is the time to act.
—President Richard Nixon, 1969[1]

Richard Nixon and Lawrence O'Brien were unlikely—and brief—allies. On September 2, 1969, President Nixon held a short press conference at his San Clemente, California, home.[2] The press conference was organized to push for a seemingly impossible task: postal reform.[3] Standing to Nixon's right, in a show of bipartisan support, was O'Brien.[4] Nixon and O'Brien did not agree on much. O'Brien was the consummate Democratic Party insider—he had run President Kennedy's Senate and presidential campaigns; had served as a special assistant for congressional relations in both the Kennedy and Johnson administrations; had headed the Democratic National Committee in 1968; had overseen the Post Office Department as postmaster general under President Johnson; and had run Robert Kennedy's ill-fated presidential campaign—and a natural adversary for Nixon.[5] Yet on the issue of postal reform, Nixon and O'Brien agreed: something had to be done. During his first term, President Nixon made postal reform a key priority. He sought to restructure the Post Office Department in a manner that would relax, if not entirely remove, political oversight and push postal service toward a more business-like footing.[6] In an effort to build support for legislative reform, Nixon successfully prodded O'Brien to cochair the Citizens Committee for Postal Reform, a newly formed lobbying organization dedicated to pursuing legislative change.[7] Like Nixon, O'Brien supported overhauling the Post Office Department. The San Clemente press conference was somewhat stilted. In his memoir, O'Brien recalls Nixon being uncertain as to whether he should call him "Larry" or "Mr. O'Brien" (he eventually settled on Larry).[8] The press conference was designed to highlight the bipartisan support for reform,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

but the cause seemed doomed, or at least, unlikely to succeed. The Post Office Department was deeply entrenched in the day-to-day life of the nation and featured a bureaucracy made up of hundreds of thousands of federal employees. Reform was not a modest goal. As O'Brien wryly remarked during the press conference, "This bipartisan effort may continue forever."[9]

Yet, despite O'Brien's skepticism, postal reform would indeed come to pass. The Postal Reorganization Act (PRA) of 1970 would transform the Post Office Department into the United States Postal Service (USPS). The act kicked off a decade of infrastructure reorganization. Across seemingly all infrastructure sectors, political controls that had appeared stable gave way and were replaced with the logic of the market. O'Brien joined President Nixon for the ceremonial signing of the reorganization bill in August 1970.[10] It was the second and last time O'Brien and Nixon would meet face-to-face.[11] Their fates, however, would again intersect. In 1972 a watchman at the Watergate complex caught burglars breaking into O'Brien's office. Agents working to reelect President Nixon had been tapping O'Brien's phone at the Democratic National Committee headquarters (O'Brien was again serving as chairman for the Democratic National Committee). The ensuing scandal would eventually lead to President Nixon's resignation in 1974.[12]

* * * *

The following chapter examines the dismantling of traditional regulatory approaches and the rise of deregulation. Beginning in the 1970s, price-and-entry regulations governing infrastructure services were dramatically, and quite unexpectedly, largely dismantled.[13] Liberalization and reform opened infrastructures to competition and relaxed state control and supervision over rates. Deregulation transformed the rules governing infrastructures that had been in place for decades (or longer). It attempted to reduce the role of the state in overseeing key aspects of infrastructure services and introduce, however imperfectly, market-based competition. These legal and policy changes led to material changes in the design and operation of infrastructures that created new (or enlarged existing) forms of risk and, equally as important, remade the relationship between the state, network operators, and various other infrastructure publics. It was against the complicated backdrop of deregulation that post-9/11 debates about infrastructure security unfolded.

Deregulation affected a broad swath of services, including the postal system, telecommunication, transportation (including, rail, trucking, and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

airline service), and electric power and was, in each instance, significant and partial. At its most basic level, the revision and in some cases rescission of regulations governing price and entry attempted to replace administrative controls with market rationality. It was a radical change. Deregulation removed infrastructures from many of the political constraints within which they had long been embedded. This transformation offered a historic repudiation of the basic compact that had attempted to strike a balance among the broad aims of social policy, heterogeneous interests, and the particular economic and technical characteristics of infrastructures. Though the dynamics of the forces driving the push for reform and the specifics of how deregulation unfolded differed across infrastructural sectors, in all instances deregulation was a political process of restructuring that sought to relax (or fully eliminate) economic regulations governing price and entry in infrastructure services in favor of a closer embrace of the market. In this fashion, deregulation was a central tenet of a larger global neoliberal transformation that undermined public institutions and faith in the possibilities of collective decision-making in favor of an uncritical celebration of the market.[14] Regulation, at its best, served to impose a counterweight to the power of the market (in incomplete and flawed ways, to be sure) and impose some degree of public accountability over these important services. Deregulation took direct aim at these forms of accountability, undermining them and leaving a new balance of power in its wake.

The following chapter revisits and reinterprets the process of deregulation within the postal industry, freight rail transportation, and electric power system. In each case, new legislation during the 1970s and 1980s greatly transformed the institutional framework governing these networks. The PRA of 1970 began the process of transforming postal service by paving the way for the partial liberalization of the postal market, phasing out direct subsidies from the federal government for general operation, and undercutting the continuation of cross-subsidies between different categories of service in a movement toward rates that more directly reflected market conditions. In rail service, the Railroad Revitalization and Regulatory Reform Act of 1976 and the Staggers Rail Act of 1980 transformed the industry by allowing shippers and carriers to set rates privately and railroads to define the outlines of the networks upon which they operate. In electric power, the Public Utility Regulatory Policies Act of 1978 (PURPA) began the tentative creation of competitive electricity markets and the splitting of local vertical monopolies controlling generation, transmission, and distribution. In each case, political

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

restructuring quickly began to rewire the organization of these networks. Power shifted and slid into a set of new configurations. Deregulation empowered particular infrastructure publics within each sector: it gave large commercial mailers a de facto veto over postal policy; it allowed railroads a somewhat free hand in setting rates and defining the outlines of their networks; and it led to the creation of a host of new important actors—including non-utility power companies and large regional coordinating bodies—in electric power. Deregulation also led to material change: operators reprioritized investment, cut redundancy, and abandoned seemingly unnecessary services. In just a few short years, newly deregulated infrastructures would look far different from their regulated predecessors. Deregulation promised to sweep away the inefficiencies of the old regulatory model to create lean infrastructures trimmed of the fat that had accumulated under state stewardship. But these changes came at a price. Reform created infrastructures that are increasingly susceptible to natural disasters, accidents, and terrorism. The drive to improve efficiency wound up creating systems that are ripe for large-scale failure. It is precisely these new possibilities of failure that would reappear post-9/11 as pressing and difficult public problems.

To understand the specifics of deregulation as it unfolded within the postal sector, freight rail system, and electric power grid, we now turn to examine each sector in detail.

Deregulating Postal Service: Modernization, Information and Communication Technologies, and Vulnerability

The U.S. postal system underwent a process of selective deregulation that began with the passage of the PRA of 1970 and subsequently unfolded in a series of administrative proceedings that stretched into the early 1980s. Initially framed as a way of removing the deleterious effects of "politics" on postal affairs and enhancing the autonomy of postal management, reorganization transferred the operation of the postal system from the cabinet-level Post Office Department to a new independent government establishment (USPS). Quickly, however, reorganization took on a life of its own. Through a series of administrative hearings and decisions, what started out as a way of empowering management morphed into something else—a movement toward deregulation. In changes that were not anticipated by reformers, postal rates were largely recast according to market factors, and large portions of the postal network were effectively liberalized. Ironically, these changes wound up circumscribing the power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

of managers in key respects and empowered well-organized commercial mailers to assume a dominant role in postal decisions. Although deregulation led to the adoption of a new, lean, and more efficient postal network, this process was not an unqualified success: these changes unwittingly injected new forms of vulnerability into postal operations and created the conditions for large-scale failure. Regulatory reform remade the postal system into a tightly coupled and complex processing network. While the previous structure of regulation supported distributed and labor-intensive processing (see chapter 1), deregulation undid these supports and subsequently led to the adoption of automation and centralized processing within a collection of dense network hubs. As the 2001 anthrax attacks would vividly highlight (see chapter 4), the successes of reorganization were not without their drawbacks.

Postal Service and the Push for Comprehensive Reform

The push to reform postal service came from postal management and leadership. By the mid-1960s, the Post Office faced an economic and operational crisis characterized by rising costs, an expanding deficit, and declines in the quality of service. Post–World War II economic prosperity fed a spike in mail volume that overtaxed the postal infrastructure: between 1945 and 1970, annual mail volume leaped from 37.9 billion to 84.8 billion pieces, and total postal costs ballooned from roughly $1.1 billion to $7.3 billion.[15] Revenue, however, did not keep pace, rising from $1.1 billion to only $6.3 billion over the same period, leading the Post Office Department to accumulate a deficit in excess of $1 billion by the late 1960s (see figure 2.1).[16] The postal network was largely ill-equipped to handle the influx of volume and service suffered. Postal equipment had not been updated in decades, and the existing network of post offices was structured around increasingly obsolete rail lines, which made offices difficult to access via the now prominent modes of truck and air transportation.[17] The dire state of affairs was given visible expression with the breakdown of the Chicago post office in 1966. As 10 million pieces of backlogged mail sat immobile in the office and in trailers lining the surrounding streets, management considered the drastic step of burning the accumulated mail in a desperate effort to "reset" the system.[18]

To Postmaster General Lawrence O'Brien, the breakdown was symptomatic of a larger looming crisis: increasing volume, rising costs and deficits, and outmoded infrastructure and technology would make large-scale breakdowns like Chicago the norm. In his estimation, the postal system was in a "race with catastrophe," and regulatory reform provided the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

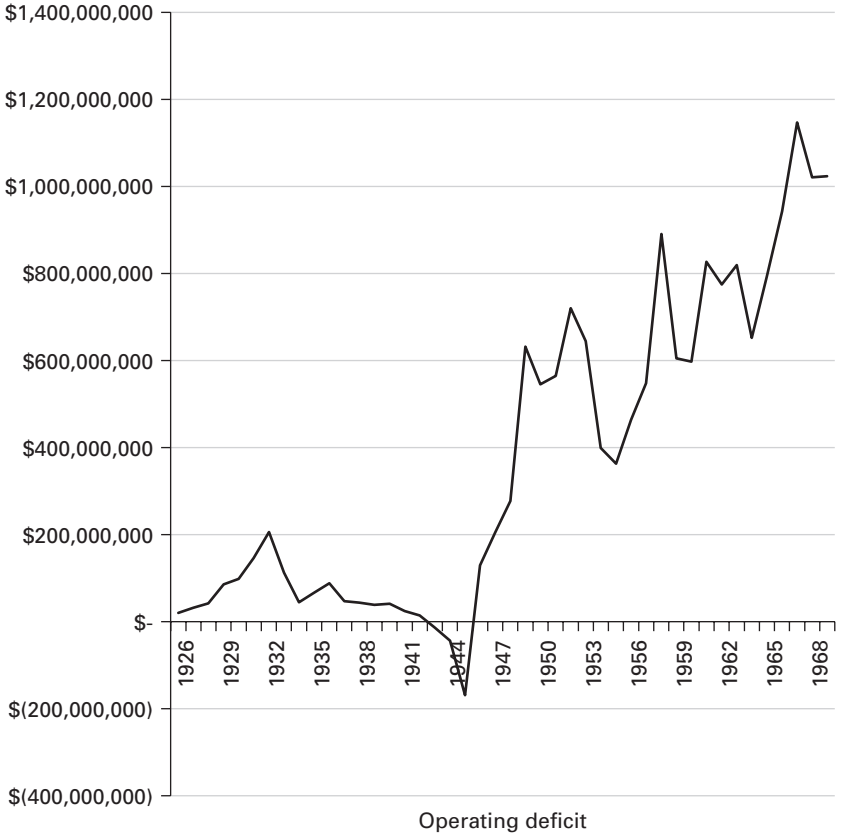


Figure 2.1
Postal operating deficit, 1926–1969. POD, *Annual Report of the Postmaster General, 1969*, 236–41, table 801.

only answer.[19] O'Brien pressed the issue of comprehensive postal reform during his tenure in office, over the reluctance of President Johnson, and secured the creation of a presidential commission to examine and offer recommendations on postal reform in 1967.[20] The commission, known as the Kappel Commission after its chairperson, former head of AT&T Frederick Kappel, released its final report in 1968 and provided the basic outlines for reform legislation.[21] As the cochair of the bipartisan Citizens Committee for Postal Reform, O'Brien was able to secure a comment in support of postal reform in President Johnson's farewell address and worked in tandem with President Nixon's postmaster general Winton Blount to advance the Kappel Commission's recommendations.[22]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Reform faced an uphill battle. The idea of reforming the basic structure of the postal system was not completely novel. Periodically, different groups had agitated for dramatic reform.[23] Nor was a postal deficit unprecedented; though the deficit spiked during the 1960s, revenue shortfalls had been the norm for over a century.[24] Historically, however, a host of complementary institutions supported the status quo and blunted calls for comprehensive change. The unique form of postal service created in fits and starts during the late 18th and 19th centuries became invested in other mutually supporting institutions. The publishing industry, political campaigns, and national voluntary associations all relied on cheap second-class postage for their operation, while political parties relied on the dispensing of local postmasterships as a key source of political patronage.[25] In each instance these interests provide a key source of "feedback" supporting the continuation of the postal status quo.[26] This mutual support, as much as ideological commitment to an ideal of service, helped ward off comprehensive reform.[27]

This matrix of support was, however, fragile and contingent. By the 1960s generous postal rates were not quite as important to publishers as they had been in previous decades. Alternate communication and distribution channels—de facto competition—eroded the significance of the postal system, particularly as a channel for news gathering. Most importantly, during the 20th century the tight connection between the postal bureaucracy and partisan politics frayed. Carriers and clerks were placed under the civil service system (as opposed to postmasters, who were still political appointees) and became an independent, unionized political force that agitated for better working conditions and wage increases.[28] The growing activism of labor transformed the relationship between partisan politics and hence Congress and postal labor: the postal workforce morphed from a political resource into a liability. By the late 1960s, postal reform appeared to be an attractive way for Congress and the executive branch to divest themselves from the headaches and diminishing benefits that flowed from involvement in postal politics.

Through tense negotiations with mailers and labor, the Nixon administration secured the passage of the PRA. Critically, postal unions, initially a key roadblock to passing reform legislation, agreed to throw their support behind reorganization in exchange for wage increases and binding arbitration.[29] Commercial mailers also came onboard once former postmaster general O'Brien, current postmaster general Blount, and the Nixon administration put their weight behind reform, and regulatory restructuring appeared to be a real possibility. The promise of reducing

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

postal costs served as a carrot for mailers leery of losing generous rates in the face of escalating costs and declining service.

The Postal Reorganization Act of 1970

The Kappel Commission's report provided the basic blueprint for the PRA. The commission identified "politics" as the problem hampering the postal system.[30] The fracturing of authority between Congress and the executive branch meant that postal managers had no control over costs, revenue, or investment (see chapter 1). In the commission's view, congressional authority to set rates was a disaster that favored political expedience over sound business discretion and economic data. The commission recommended transforming the Post Office Department into an independent, self-supporting corporation owned by the federal government. The postal corporation, as the commission called it, would be free to open and close offices; set rates in accordance with sound data; study, borrow, and invest in new technologies; and operate with the efficiency and flexibility of a business. Postal management would be allowed to actually manage. The Kappel Commission argued that the reorganization of postal service into a business-like model would lead to the elimination of the postal deficit, lower rates, and improved service.[31] While the commission did not explicitly favor the repeal of the postal monopoly, it did advocate that management should have a greater hand in determining rates and service.[32]

The commission's recommendations were written into law as the PRA. The PRA abolished the cabinet-level Post Office Department and established USPS as an independent government agency and the Postal Rate Commission (PRC), a body to review postal rates and offer recommendations. The PRA also began the process of phasing out federal appropriations and required USPS to break even.[33] A new Board of Governors would head USPS and be subject to staggered appointment (to ensure that no single president could stack the board).[34] USPS would operate with little direct congressional oversight; it could initiate rate increases, borrow up to $15 billion, invest in new technologies and improvements as it saw fit, and, it appeared, generally operate with a more or less free hand. Some general language, however, was written into the law noting the importance of rural service, equitable rates, and the continued support for cultural, literary, and informational content. Finally, the new PRC was to serve as a board of review to ensure that rates were fair, based on evidence, and set in accordance with the aims of the PRA.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The Politics of Postal Rates: Cost, Cross-Subsidies, and Value

The PRA transformed the basic outlines of postal governance by shifting authority from Congress to the newly created USPS. This transfer was intended to remake postal service in the guise of a typical business enterprise that could invest in new technologies, set rates, and define service at the discretion of the Board of Governors. Yet the PRA included vague language acknowledging that the Postal Service did, indeed, have a public service mission and retained the Private Express Statutes (the laws that provided a government monopoly over postal service). Sorting out how to reconcile these different aspects of postal service—how USPS would function as a business *and* a public service—was left muddled by the PRA. It would eventually be worked out through a series of contentious landmark rate cases and administrative hearings during the 1970s and early 1980s.[35] The PRA did not, to be clear, eliminate politics from postal affairs; rather, it changed the venue within which different interest groups, including mailers and labor, fought over the manifestly political issues relating to cost and terms of service. Now, these debates occurred through formal rate cases and administrative hearings that featured arcane economic studies and precise legal justifications. It was here that the process of deregulation proceeded. Within these hearings and cases, a coalition of large-volume mailers attacked and helped discredit what had been the cornerstone of postal regulation for over a century, cross-subsidies between different forms of content, in favor of market prices. These attacks were enormously successful: they led not only to the transformation of how postal rates were thought of and designed but also to the liberalization of large portions of the postal network and the granting of a de facto veto for large-volume mailers in determining postal policy. In the drab language of economic theory and legal minutiae, substantial and dramatic changes to the constitution of postal service occurred. Congress had been an imperfect way of imposing public accountability upon the postal system. But deregulation would shift power toward large commercial mailers. Reform was supposed to empower management, but this proved elusive. The rejection of cross-subsidies introduced new notions of discriminatory pricing into the setting of postal rates that in turn limited managerial autonomy. The impact would be far-reaching, affecting the Postal Service's adoption of new information and communication technologies (ICTs) and, more broadly, the balance of power within postal politics.

The PRA established an ambiguous set of guidelines for determining rates and classifications. It phased out direct appropriations and stated in part that "each class of mail or type of mail service bear the direct and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

indirect postal costs attributable to that class or type plus that portion of all other costs of the Postal Service reasonably assignable to such class or type." It further states that "the value of the mail service actually provided each class or type of mail service to both the sender and recipient" should be a factor in setting rates.[36] In other words, both cost and "value" are to be used in setting rates. However, it was initially unclear how costs would be determined (how attributable costs would be ascertained and the remaining assignable costs proportioned) and what would define value. Resolving these issues was central to the first several rate cases inaugurated under the PRA.

Immediately, during the first case (R71-1) instituted in 1971, different coalitions of mailers began challenging the Board of Governors' allocation of costs and corresponding proposed rates.[37] The debate in this and in subsequent cases centered around two questions: (1) the method used to determine attributable costs (those costs directly related, and thus charged, to a class of mail); (2) the logic or method of fixing assignable costs (those shared institutional costs to be divided across the classes).[38] The Board of Governors (with the support of publishers of newspapers, magazines, and other forms of second-class mail) in effect proposed to maintain cross-subsidies using a short-run costing methodology to determine cost attribution and *inverse elasticity* and value-of-service justifications for assigning costs.[39] The USPS model of short-run costs was defined as attributable costs that directly fluctuated with changes in volume. This left a significant amount of postal costs (51% during the first rate case; 55% in the next) as institutional or common costs. This approach would have preserved a significant amount of discretion for the Board of Governors in setting rates: the remaining institutional costs could have been assigned to classes of mail according to elasticity (the degree to which volume fluctuates with changes in rates) and the presumed public importance of content.[40] Under this approach, the old model of postal rates—in which cross-subsidies worked between different types of content, with letters defraying the costs of newspapers and magazines, for example—could have been preserved.

The Board of Governors faced significant pushback. The postal system divided mail into a number of different categories: generally, first-class mail included sealed personal correspondence, such as letters and bills; second-class mail included magazines and newspapers; and third-class mail included, most significantly, advertising circulars. Interest groups representing first-class mailers (the Association of Public Utility Mailers and the National Association of Greeting Card Producers, most prominently)

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and third-class mailers (such as the Association of Third Class Mailers and the Mail Advertisers Service Association) challenged the postal Board of Governors.[41] They pointed out that the PRA called for rates that supported *all* of the costs that could be attributed to a particular class of mail and only a *reasonable* share of the remaining (assignable) coasts. First- and third-class interveners advocated a method of long-run costing that attributed nearly all costs. Under this approach, postal management would find their hands tied. There would be little room for discretion or for the continuation of cross-subsidies between types of content. According to this model, first- and third-class rates would decline, while second-class rates would dramatically increase. First-class mailers argued that they were a "captured" class of mail. First-class mail is subject to monopoly restriction (other classes are not): only the government can carry and deliver it. For first-class mailing interests, the proposed postal rates under the terms of the PRA were unfair. Using inverse elastic pricing, in their view, punished them: the monopoly class of mail—letters—would always be less sensitive to cost fluctuations than other mail matter and, as a result, would wind up shouldering the burden of institutional costs. First-class mailers, accordingly, argued that such a pricing scheme violated the terms of the PRA. Third-class mailers also argued that by adopting the Board of Governors' preferred short-run costing methodology, third-class rates were greatly inflated (due to paying for other forms of service). Both argued that rates should, in effect, have nothing to do with the value of the content carried in different classes of mail.[42] That is, demand, and not assumptions of the broader importance of the content of certain types of mailings, should serve to define value under the PRA. The market, not substantive judgments by postal management, should evaluate worth. Taken as a whole, these interveners argued that cross-subsidies and redistribution had no place in postal service and that managerial discretion should be limited to the greatest extent possible. They advocated strict cost-of-service considerations as the single factor in setting rates and fought against interpreting the value-of-service provision of the PRA as supporting preferred content.[43]

Disputes over cost attribution and assignability were about the linked concepts of the Board of Governors' autonomy, the validity of cross-subsidies, and the meaning of value in determining rates; they were about substantive regulation and its role in the organization of the postal market. In each of the first three rate cases, the same problems appeared. The presiding administrative law judge and the PRC accepted the basic outlines of the arguments of first- and third-class mailers and pushed the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Board of Governors to develop models accounting for greater portions of costs (and thus limit the discretionary power of management). The Board of Governors did so reluctantly, but refused to assign all costs; the subsidies were reduced but not completely abolished.[44] Second-class rates rose significantly, but the Board of Governors maintained some limited discretion over rates.[45] Although the more radical proposals to have full-cost accounting shape rates and to use only demand factors (i.e., fluctuations of volume) as the guides to value were averted, cost become *the* major factor in shaping rates.[46] More importantly, first- and third-class mailers were able to formally introduce antitrust principles and apply them to the setting of rates for all classes of mail.[47] The foundational premise of reorganization, to give the postal bureaucracy increased autonomy and control, was quickly dashed; the redistributive system of cross-subsidies was successfully challenged, and the ability of the state to assign different rates based on distinctions of the value of content was greatly reduced.[48]

New Technologies and New Opportunities: The Postal System and the Information Revolution

The introduction of new notions of nondiscriminatory pricing into the setting of postal rates and the discrediting of cross-subsidies were important victories for large-volume mailers. In addition to lessening the share of costs shouldered by first- and third-class mailers, the outcome of the early rate cases provided mailers with new power to dictate the direction of postal policy. Postal reorganization was designed in large part to aid management's adoption of new technologies and increase their control over key terms of service. Under the PRA, the new USPS was promised the autonomy to raise capital through self-supporting rates and borrowing and invest as it saw fit. Yet the successful introduction of principles of nondiscriminatory pricing and the attack on cross-subsidies circumscribed this autonomy. Now, large-volume mailers were able to essentially wield a veto over postal policy. By raising the objection that monopoly revenue generated through first-class rates subsidized other forms of service, which resulted in both an unfair tax on the captured class of mailers and unfairly subsidized Postal Service activity in ostensibly competitive markets (such as electronic mail, as discussed below), large-volume mailers were able to dictate postal policy as they saw fit.

During the 1970s, mailers quickly seized on the discrediting of cross-subsidies and the new centrality of cost in the setting of rates to successfully argue for the partial liberalization of the postal network. Mailers pushed through new work-share discounts that allowed them to receive

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

lower postal rates for presorted mail. In effect, these new workshare discounts reduced the reach of the postal monopoly to the last mile. These new discounts allowed bulk mailers and new third-party presort aggregators (specialized companies that compiled and bundled business mailings for clients for a fee) to deliver prepared mailings to select postal facilities close to their final destinations at reduced rates.[49]

Importantly, mailers further used their newfound power to dictate the terms on which the Postal Service would—and would not—adopt new ICTs. Through the 1970s and 1980s, the Postal Service pursued two strategies concerning new ICTs: market growth and expansion through the introduction of an electronic mail system, a proto-email service dubbed E-COM (electronic computer originated mail); and cost reduction and improved efficiency through increased reliance on mechanization and automation. Mailers, in direct conflict with the wishes of postal management, pushed the Postal Service to abandon efforts to use ICTs for a hybrid "electronic mail service" and supported the use of new technologies as a means of controlling costs and improving the efficiency of the basic postal network. By steering postal management away from innovative new forms of service and toward a program of internal improvements structured around mechanization and automation, large-volume mailers helped to create a tightly coupled and complex processing network.

An Electronic Postal System? The Failure of E-COM

USPS proposed E-COM in 1978 as a means of countering the long-term forecasted electronic diversion of hard copy mail by new forms of electronic communication. By the middle of the 1970s, it became clear to postal management that new low-cost electronic message systems (EMS) and electronic funds transfer (EFT)—including automated clearinghouse networks, point-of-sale networks, and automated banking systems—threatened the viability of the postal system. Managers feared that electronic diversion would siphon off the low-cost, high-volume business market that produced the bulk of postal revenue and eventually cut into the use of first-class mail for personal communication. Unchecked, these new systems would service lucrative markets first, leaving the postal system with diminishing returns and the continued obligation to serve those left out.[50] The Board of Governors' request to alter the mail classification schedule outlined E-COM as an electronic/print hybrid that would integrate electronic transmission and data processing with the delivery of print letters.[51] Under the proposed plan, USPS would contract with a telecommunications carrier to provide service between 25 *serving post offices*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

(SPOs) and a designated point of reception. Once an electronic message was sent to the service, it would be forwarded to one of the SPOs (in electronic form), printed, enveloped, and delivered. USPS would be acting as a telecom reseller, leasing telecom services from a provider (such as Western Union) and bundling electronic transmission service with data processing and letter delivery as a single product sold to a consumer.[52] E-COM was intended to be a first cautious step in providing electronic mail services, with the possibility of more expanded, fully electronic transmission and delivery to follow.[53]

Large-volume mailers and telecom companies quickly undermined E-COM and ensured its failure.[54] During the PRC review of the proposal, associations of first-class mailers (including utility companies and greeting card manufacturers) and private telecom companies (such as Graphnet Systems, MCI, Xerox, AT&T, and a host of others) argued that the new service would invariably and unfairly be subsidized with revenue from first-class rates, making such rates discriminatory by taxing regular users of first-class mail to support this risky and costly new venture. This would give the Postal Service an unfair leg up in competing with private telecom providers of similar electronic communications services.[55] That is, they charged that the capital-intensive E-COM would both unfairly burden first-class mailers and place private telecom services at a competitive disadvantage.[56] In response to these arguments, the PRC radically reconfigured the Postal Service's proposal. In its place, it outlined a reworked E-COM service that was doomed to fail.[57] Under the PRC's alternative E-COM plan, USPS had no control over the electronic transmission of messages, the costs of service would be borne fully by users of the service (cross-subsidies would not be allowed), and the total operational and start-up costs had to be recovered quite early, during the third and fourth years of the service's operation.[58] These changes all but ensured that E-COM would be dead on arrival. The reworked E-COM went live on January 2, 1982, and despite a steady growth in volume, it operated for slightly over two years before being discontinued.[59] The move to separate electronic transmissions resulted in high transmission costs, and the requirement to recover all costs during the third and fourth year led the PRC to set 200%–300% increases in rates for 1984.[60] The Postal Service surmised that the rate hikes would be fatal to the service and, rather than raising rates, abandoned the service. Alas, the future of the Postal Service would not involve email.[61]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Mechanization and Automation: Centralized Processing and ICTs

While large-volume mailers and their associated allies used arguments about unfair competition and discriminatory pricing to prevent USPS from capitalizing on the emerging electronic communication market, the Postal Service did adopt new forms of ICTs for the purpose of processing mail. Mechanization and automation became regular features of postal service during the 1970s and 1980s. The Postal Service invested over $6 billion in new equipment after reorganization. The adoption of new forms of mechanization and automation transformed the postal network.

The Postal Service first invested heavily in mechanization before turning, in the early 1980s, toward automation. During the 1970s the Postal Service invested over $1 billion in new mechanized equipment, mainly multiposition letter-sorting machines and single-position letter-sorting machines (MPLSMs and SPLSMs), to help control labor costs. Sorting mail was labor-intensive. During the year before regulatory reform, a mere 10% of total letters were processed on mechanized equipment. By the 1980s, however, the Postal Service's commitment showed real progress, as 80% of total mail was now processed by mechanized equipment (see figure 2.2).[62]

Automation followed in earnest during the early 1980s. The old Post Office Department provided meager initial research and development funding to Philco and IBM during the 1960s for what would become the central technology in automating postal sorting and handling: optical character readers (OCRs).[63] OCRs perform a number of operations: they scan letters (or other material), "read" the address written on the piece, translate this information into a bar code, and spray the bar code on the

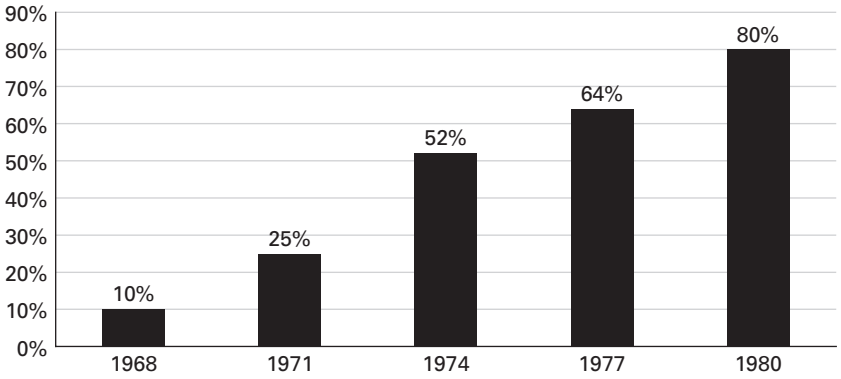


Figure 2.2
Percentage of USPS mail volume sorted mechanically, 1968–1980. Cortada, *Digital Hand*, 169; Biggart, "Post Office as a Business," 487; POD, *Postal Progress*, 7.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

piece for later sorting. Once bar coded, bar code sorter (BCS) machines scan the code and sort the mail for distribution. The Kappel Commission discussed automation in its report as a possible key source of cost reduction.[64] But it was not until the deputy postmaster general's Task Force on Mail Processing Systems offered its recommendations in 1976 that a clear automation strategy was developed.[65] USPS invested $5 billion into new automation equipment between 1980 and 1997, eventually acquiring over 13,000 pieces of hardware.[66] The Postal Service rolled out first-generation OCRs in 1982 and updated versions, known as multiline OCRs, or MLOCRs, in 1988.[67] The key difference between these two systems relates to the amount of information that can be read and synthesized. While the earlier OCRs only read the lowest address line (including city, state, and zip code), MLOCRs read the entire address, match the address against an electronic database containing a compilation of address information (names and addresses), and then apply a bar code containing the relevant information. Video cameras take snapshots of letters that cannot be processed by MLOCRs (due to illegible handwriting or other forms of presentation that cannot be identified) and transmit the image to remote encoding centers, where operators read the address, manually input a bar code, and transmit the data back to the sorting facility, where it is printed on the letter.[68] MLOCRs and remote encoding centers allow for a greater degree of depth in sorting and enable the organization of mail into delivery sequence (known as delivery point sequence, or DPS) without repeated sorting and resorting throughout the network.[69]

The Postal Service's commitment to and investment in mechanization and automation reflected its autonomy from the strictures of congressional oversight—*and* its subservience to large-volume mailers. Congress had now taken a back seat in trying to balance the different priorities and publics that clung to the postal system. Large-volume mailers now dominated postal politics. Importantly, unlike with E-COM, commercial mailers did not voice strong opposition to internal improvements designed to lower processing costs. The $6 billion investment undertaken between 1970 and 1997 dwarfed any comparable investment undertaken by the Post Office Department under congressional supervision. Between 1955, when modernization efforts first got off the ground, and 1968, the Post Office Department invested $520 million *total* in large capital programs, including mechanization, automation, and new facilities and other equipment. Of this amount only a paltry $173 million was devoted to mechanization and automation.[70] Though revenue and expenses also rose sharply after reorganization—the Postal Service by the late 1970s

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

was dealing with significantly more mail, revenue, and expenses than the previous Post Office Department—the commitment toward automation and mechanization as a percentage of total annual obligations showed a dramatic and telling increase. Between 1955 and 1968, the Post Office spent, on average, .38% of its total obligations on mechanization and automation annually, while between 1970 and 1997 the Postal Service devoted an average of .77% of annual total obligations to mechanization and automation.[71]

Mechanization and automation helped improve productivity and efficiency as postal volume exploded. New technology sped up the throughput of mail processing and reduced the number of workers needed to process the mail. Manual sorting processes 600 pieces per hour, mechanized sorting increases the rate to 2,800 per hour, and OCRs sort letters at a rate of roughly 30,000 per hour.[72] In 1970 the Post Office Department processed 85 billion letters with a workforce of slightly over 501,000 employees—a rate of 167,000 pieces of mail per employee. By 1995 USPS carried 180 billion pieces of mail with roughly 875,000 workers—a rate of 206,552 pieces of mail per employee.[73] Automation and mechanization helped reduce the number of clerks employed, dropping from 308,000 and 42% of total workers in 1968 to 274,000 and 31% of total workers in 1995. By the middle of the 1990s, the Postal Service was processing over 659,000 letters annually per clerk employed, compared against roughly 275,000 letters per clerk during the late 1960s.[74] Automation and mechanization both reduced the total number of workers needed and, importantly, reduced the number of full-time career workers. Previously, sorting the mail relied on knowledgeable clerks (occasionally aided by mechanized "keying" equipment) and carriers to recall addresses, zip codes, and other data for disambiguation.[75] Automated sorting deskilled the work of clerks (in sorting the mail for distribution between offices) and carriers (in having to correctly sort letters for delivery). Specialized knowledge about routes, addresses, and the like became less essential. New technology allowed temporary workers to approximate the performance of career employees.[76] Finally, new technologies helped reduce unit costs when adjusted for inflation. It cost $42 to manually sort 1,000 letters; these costs dropped to $19 per 1,000 with mechanization and $3 per 1,000 with automation.[77] In 1970 it cost the Post Office $.35 in adjusted 1995 figures per piece of mail, while in 1995 unit costs were only $.28.[78]

The adoption of automation transformed the material organization of the postal network. The addition of new technologies required the centralization of sorting and processing.[79] While political pressure forced (and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

largely continues to force) USPS to maintain an expansive (and expensive) network of retail post offices, the internal network has been consolidated. Since reorganization, sorting and processing have become the province of a dwindling number of critical hubs.[80] Before reorganization, the Post Office Department divided the country into 552 substate districts, each containing a sectional center that served as a processing and distribution hub that linked to surrounding post offices (from which mail was collected, sorted, and delivered) as well as other sectional centers.[81] By 2001 the sectional centers had been roughly halved into 237 Processing and Distribution Centers (P&DCs). These facilities serve as the key points in transit for mail as it moves through the postal system and as entry points where bulk mail is comingled with the general mailstream.[82] The pursuit of efficiencies provided by centralizing processing and handling in P&DCs reconfigured the postal network into a more tightly integrated spoke-and-hub design.[83] These centralized facilities now are the critical hubs that link roughly 40,000 post offices, 350,000 collection boxes, and 136 million unique delivery addresses into a national network that processes 680 million pieces of mail daily.[84] Individually, P&DCs sit as the gateways into large cities and regions and connect local post offices with the broader postal network.[85]

The Triumph of Large-Volume Mailers: The Deregulation of Postal Service

The remade postal service is an example of selective and incomplete deregulation. While the letter monopoly still exists and USPS is a public entity, substantive regulation is largely absent. The equation of rates with market forces is at odds with the foundational ethos of postal service that made explicit the aim to provide services in excess of what the market would provide. Currently, the service is in a precarious position: automation and the explosion of ad mail, which fed the phenomenal growth in volume during the 1980s and 1990s, provided some cover, but long-term trends suggest a dire position. Costs continue to rise, while volume, finally, appears to be stalling and actually falling. These trends will serve to empower large-volume mailers all the more. As other users and customers fall away, commercial mailers become increasingly central to the service and, as a result, all the more powerful.[86]

Despite the failure of E-COM, the postal service was not completely shut out of the information revolution. Regulatory reform did enable postal management to adopt new ICTs into their operation. But the ethos of deregulation guided and limited precisely how these new technologies

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

would be used, ultimately pushing the Postal Service to use ICTs as a tool to streamline the processing network while blocking expansion into growing electronic communications markets. Mechanization and automation provided some clear productivity and efficiency gains. The deployment of new ICTs advanced in tandem with the recalibration of the postal network into a more tightly integrated hub-and-spoke network structured around P&DCs in order to capture the newfound economies associated with increased throughput and lower unit costs.

The Limitations of Centralized Processing

The reorganization of the postal network into a system of interlocking, dense processing hubs has, without question, improved efficiency. Over the past several decades, postal volume has sharply risen while costs and levels of service have remained fairly consistent or improved. As a result of automation, more mail is now processed more quickly in fewer locations at a comparatively lower price. Yet, while the benefits of automation—and by extension of regulatory reform—are plain, improved efficiency is not without its costs. By moving from a distributed to a centralized model, the postal network now is more vulnerable to infrequent large-scale failure. While random failures at single points within the network are, for the most part, of little concern, a failure that occurs within a dense hub can have an inversely large impact on the larger network. For example, the random disruption of mail service along any single postal route, home, or even branch office would not in all likelihood affect the larger network. The failure would be minor and relatively trivial. Yet a failure at one of the approximately 200 processing hubs that now make up the backbone of postal service would not be trivial. The postal system is tightly yoked together and reliant on complex automated technologies that sort mail into ever-fine-grained distributions. Letters move faster than ever through processing machines located at a small number of facilities. These facilities, and these machines, are central to the entire network. Failures here can quickly spin out across the entire network. Centralized processing plants create choke points where failures have the possibility of affecting a large number of connected users (i.e., those linked to and served by the incoming and outgoing mail flows of the plant).[87] The aggregation of processing activities in fewer locations and the reliance on machines that sort mail for ever-greater sets of destinations create new interdependencies within the network. These interdependencies create the conditions for large-scale failure or, as Perrow would describe, normal accidents. The old model of labor-intensive processing was costly, slow, and redundant.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Workers repeatedly sorted mail in a step-by-step fashion across a number of different facilities around the country. This provided a degree of slack and redundancy that is now missing. While reform created a more efficient postal service, it also created the new possibility of systemic failure, which had been largely absent. The possibility of such a failure, however, ceased to be purely theoretical during the 2001 anthrax attacks (see chapter 4).

Railroad Deregulation: Salvation and Risk

As outlined in chapter 1, ICC regulation of freight transportation enacted a compromise between various infrastructure publics. Shippers, railroads, and consumers each benefited from the stability and quid pro quo of ICC-led regulation. Regulation also provided a measure of resilience. Though largely as an unintended side effect, the structure of freight regulation discouraged the shipment of large quantities of dangerous chemicals in proximity to densely populated areas. Freight regulation supported resilience through two means: (1) it helped drive the adoption of smaller shipments of dangerous materials carried by trucks and reduce bulk rail shipments; (2) it provided a circuitous rail network through which residual rail shipments could potentially move outside of densely populated areas.

During the 1970s and early 1980s, however, deregulation upended the rail economy. Reforms gave railroads greater freedom to both set rates and consolidate track. Similar to the changes in the postal system, deregulation led to the creation of a more efficient network. In the ensuing years, the scope of the rail network was radically reduced, and patterns of intermodal commodity distribution shifted, leading to a spike in the volume of large quantities of dangerous materials moving by rail. Deregulation, unquestionably, saved the failing railroad industry by allowing railroads to shed costly track and recapture traffic that had been diverted to other modes of transportation. But increased efficiency came at a price: deregulation undermined the overlooked and incidental security benefits that were intermixed with regulation.

The Push for Rail Deregulation

The process of deregulation unfolded through a series of new laws and administrative decisions during the 1970s that culminated in the Staggers Rail Act of 1980. Deregulation upended the status quo of freight regulation. It granted railroads wide latitude to set competitive rates and determine the scale of the networks they operated. The push for deregulation came largely from the railroads themselves. Widespread economic challenges eroded the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

positive benefits that railroads had long secured through regulation. At the same time, while well-publicized criticisms from a cross section of right-wing and liberal-left observers increasingly painted regulation as both anti-business *and* anti-consumer.

The push for deregulation was startling: For decades the railroads were the fiercest supporters of ICC authority and the continuation of regulations. Likewise, consensus between the ICC, shippers, and Congress historically buttressed the status quo. Indeed, for a time regulation worked well in securing tangible benefits for the railroad industry and the public. Yet by the 1970s, regulation appeared to be a bust. The steady introduction of intermodal competition—the rise of trucking, most significantly—offered cheaper and more attractive shipping options. In time, this eroded rail profits. At the same moment, economists attacked regulation as an inefficient relic, while liberal-left consumer advocates challenged regulation as a form of corporate welfare. It was against this complicated backdrop that rail deregulation unfolded.

The Durability of Freight Regulation

ICC regulation historically provided clear and obvious benefits for railroads. Price-and-entry controls protected railroads from destructive competition and the vagaries of regulation on a state-by-state basis and guaranteed a generous rate of return. At the same time, regulation was not simply a proxy for railroad interests. It also provided shippers, consumers, merchants, and the larger public with clear benefits. Regulation protected shippers from discriminatory rates and unfettered rent seeking on monopoly lines and maintained an expansive network that provided the public with access to a national system of freight transportation. Under value-of-service pricing and the general system of cross-subsidies, certain shippers and segments of the population benefited more than others, to be sure—farmers and shippers of cheap bulk products received rates that were quite low when compared against expensive manufactured goods, and the maintenance of an extensive rail system was a boon to rural interests—but in general ICC regulation of freight transportation provided broad benefits to both railroads and the larger public.[88]

Railroads, key shippers, and the ICC in turn supported the continuation and at times extension of ICC regulation. In the face of periodic challenges, the railroads were staunch advocates and protectors of ICC authority.[89] Shipping interests, particularly farmers and the U.S. Department of Agriculture (USDA), also supported the continuation and extension of ICC regulation.[90] Finally, the ICC itself became an interest group

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

wedded to and protective of the status quo.[91] In a familiar pattern, regulation encased in law became subject to self-reinforcing mechanisms that helped ensure its durability. In a crude calculus, regulation and the ICC supported railroads and shippers while railroads and shippers supported regulation and the ICC.

Cracks in the Consensus: Competition and Regulation

The deregulation of the postal system was something of a surprise—a set of pro-management policy reforms that took on a life of their own within administrative hearings—railroad deregulation was a deliberate transformation. The introduction of competition from (mainly) trucks destabilized the system of freight regulation. Cross-subsidies and value-of-service pricing function well in monopoly markets with little opportunity for consumer exit. By securing a large market and limiting alternative options, the added costs of regulation are spread across a large number of users, and customers are compelled to pay only a relatively small markup. The introduction of competition undermines this system. Cross-subsidies and value-of-service pricing create incentives for users to opt out of the regulated system in favor of services that are not saddled with added cost burdens due to an absence of regulation or a comparatively smaller markup. As customers flee to other services, the system of regulation becomes increasingly tenuous: operators are left with low-value customers and are forced to now spread costs across a smaller fraction of customers, in turn creating even greater incentives for customers to opt out.[92]

This pattern played out in freight rail. The growth of trucking services led to the substitution of traffic from rail to trucks. Trucks were a particularly attractive option for high-value manufactured goods that shouldered the greatest markup under value-of-service pricing.[93] The railroads, in concert with large trucking firms and unionized labor leery of hit-and-run competition from smaller outfits, successfully urged the extension of ICC regulation over motor carriage.[94] For the railroads, placing trucking within the ICC's ambit attempted to secure their market position and preserve the current rate structure. The Motor Carriers Act of 1935 extended ICC regulation of entry and rates to motor carriage but contained a number of exemptions that in time proved significant. As a concession to farming interests, the act exempted the motor carriage of unprocessed farm products—fruits, vegetables, and livestock—from ICC regulation. Additionally, the act only covered common carriers and exempted private carriers and contract carriers.[95] Under the Motor Carriers Act, the ICC sought to maintain the viability of the railroads and trucking through rate parity.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

That is, the ICC attempted to maintain the basic structure of rates by preventing either mode from drastically slashing prices in intermodal competition.[96] The exemptions, however, proved all-important. A thriving trucking sector operating outside of regulatory constraints siphoned freight traffic from rail service and steadily sliced into the share held by rail.[97] The ICC's attempt to protect railroads via rate parity, ironically, hastened the shift from rail to trucks. Rail had a real advantage in terms of cost over trucks for long-haul shipments. However, the ICC's devotion to parity prevented railroads from competing on price and forced them into service competition. In service competition, the flexibility of trucks offered a clear advantage that rail could not easily beat.[98]

The impact of competition on the health of railroads was stark. In 1935, railroads carried 75% of all intercity freight, but by the late 1970s, that number slipped by nearly two-thirds, to a low of 27%.[99] Trucking increased sharply during this period, and a sizable share—above 40% by the 1970s—was exempt from regulation.[100] As traffic declined, railroad profits plummeted. During the 1940s, return on investment in the rail industry averaged a decent 4.1%. By the late 1970s, the return on investment had fallen to 2%—showing profits lower than any other major U.S. industry (see figure 2.3).[101] Bankruptcy threatened to sink the national rail network. By the late 1960s and early 1970s, the situation was dire: nearly a quarter of total track was in bankruptcy, and key major lines in the Northeast and Middle West, including Penn Central, Milwaukee Railroad, and Rock Island, plunged into bankruptcy.[102] Railroads, long advocates of regulation, now became vocal champions for deregulation as a means of salvaging the industry from ruin. Through the 1970s, railroads lobbied for deregulation. The newly (1970) formed Committee for Efficient Transportation (COMET), renamed the Committee Urging Regulatory Reform for Efficient National Transportation (CURRENT) in 1975, agitated for increased freedoms to set rates and abandon track.[103]

At the same moment that intermodal competition wreaked havoc on the rail system, observers from across the political spectrum began to revisit the role of the ICC and the desirability of regulation. A series of high-profile works challenged the effectiveness and necessity of regulation under the ICC. Beginning in 1959, with John R. Meyer and colleagues' *The Economics of Competition in the Transportation Industries*, a steady stream of economic studies argued that ICC regulation caused the railroad industry to lag behind other industries, inflated prices and cut into profits, and led to the inefficient use of transportation facilities.[104] Studies in the 1960s and 1970s estimated that the yoke of unprofitable track

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

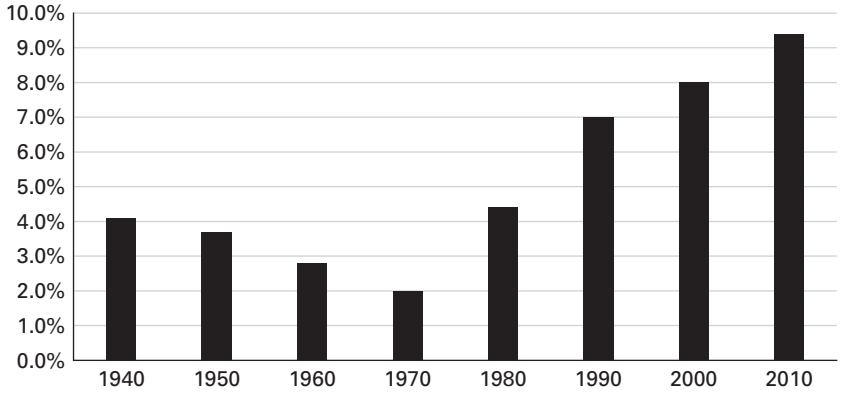


Figure 2.3
Average return on investment per decade, railroad industry, 1940–2010s. AAR, "Short History of U.S. Freight Railroads."

associated with the ICC regulation of freight railroads led to $1 billion in waste annually.[105] The rates charged by unregulated trucking services provided ample evidence of the limitations of regulation. Unregulated or exempt carriers charged rates that were between 10% to 36% less than comparable regulated shipments.[106] In 1970, Robert C. Fellmeth's high-profile and sensational *The Interstate Commerce Omission*, published under the imprint of the Ralph Nader Study Group, attacked the ICC as an example of a regulatory agency "captured" by industry that served the interests of the railroads at the expense of the public.[107] Paired with Gabriel Kolko's then recent revisionist history, *Railroads and Regulation, 1877–1916* (1965), these works charged that regulation did not ensure the public interest as much as thwart it.[108] Criticism from both the Left and Right argued that regulation, once seen as a basic solution to the unique economic problems posed by characteristics of the rail industry, was at best an outmoded relic that now promoted inefficiency and at worst the handmaiden of an industry it was ostensibly designed to regulate. These criticisms found sympathy in Congress and the executive branch beginning with the election of President Kennedy.[109] By the late 1960s and early 1970s, regulation appeared *both* anti-industry and anti-consumer. During the presidential campaign of 1976, Jimmy Carter seized on the issue as a key part of his platform, promising to undertake the deregulation of transportation.[110] *Deregulation*, as a policy option, was firmly ingrained in mainstream policy discussions.[111]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The Deregulation of Freight Railroad Transportation

The deregulation of freight rail transportation proceeded through new legislation and, to an extent, administrative decisions. In the immediate wake of the failure of rail lines in the Northeast, Congress passed the Regional Rail Revitalization Act of 1973 (known as 3R) to reorganize the seven bankrupt lines into what would be known as the Consolidated Rail Corporation (Conrail).[112] Sweeping reform and deregulation followed with the Railroad Revitalization and Regulatory Reform Act of 1976, or 4(R), and the Staggers Rail Act of 1980. The 4(R) act specified that just and reasonable rates would now only have to be equal to or greater than the variable cost of providing service. Additionally, the act specified that rates would not be considered excessive unless conditions of market dominance—that is, a lack of competition—were found. Finally, the act also granted railroads the ability to adjust rates by 7% (the "yo-yo" provision) within a given year without onerous hearings. It also provided the ICC with the power to exempt portions of service if, in their estimation, regulations would be an undue burden and serve little useful public purpose.[113]

After 4(R), the ICC used its newfound powers to further deregulate portions of freight transportation. In 1978, in response to a request from Southern Pacific Railroad, the ICC unanimously voted to remove regulation over rates for fruits and vegetables, commodities exempt from regulation when carried by trucks. The ICC also began to allow contract rates, private rates negotiated between shipper and carrier, in certain limited situations.[114]

Staggers went even further. It allowed railroads to set competitive rates and eliminate underperforming track. Staggers exempted two-thirds of *all* rates from max rate regulation, and in cases in which railroads had market dominance, rates could be set at 160% of variable cost (with provisions to eventually escalate to 180%). The act provided a greatly narrowed definition of market dominance that placed the burden on shippers to prove captivity. Contract rates were now explicitly made legal. These changes baldly benefited the railroads. Importantly, the policy on abandonments was also changed in favor of the railroads. Under Staggers, the ICC was now directed to rule on abandonments—petitions to discontinue little-used track—within 75 days if uncontested and within 225 days if requiring an investigation.[115] Previously, there were no limits on the length of time governing rulings, and hearings averaged a sluggish 400 days.[116] Staggers was the culmination of nearly a decade's work to relax regulation. These reforms reordered the landscape within which railroads operated. Regulation had, for years, worked to preserve underperforming track and had

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

established a complicated system of cross-subsidies that were supported by value-of-service pricing. These hallmarks of regulation fell away—railroads and key shippers were now in a powerful position. Now, for the first time in nearly a century, railroads had the ability to set rates in competitive markets and define the scope of their networks largely as they saw fit. Although they had greater discretion in setting prices and terms of service, they were not completely unfettered: the railroads remained common carriers and could not outright refuse service.

After Staggers: Railroads Revitalized

The sweeping regulatory changes that crested with Staggers saved the rail industry. The relaxation of control over abandonments and rates allowed the rail industry to eliminate unprofitable track, recapture significant traffic volume, and pull back from the brink of ruin. In the decades following Staggers, total U.S. rail mileage sharply declined from 200,000 miles at the close of the 1970s to 140,000 miles by 2014, levels comparable to the rail network of the 1880s.[117] The most significant declines resulted from Class I railroads (the largest railroads) abandoning one-third of total track, reducing the mileage they operated from roughly 150,000 to 94,000 miles between 1980 and 2014.[118] The reduction of the expansive network eliminated the maintenance costs associated with nonremunerative track and helped railroads reduce operating costs by nearly 60%.[119] No longer saddled with unprofitable lines or obligated to build cross-subsidies into rates, railroads successfully reversed decades-long traffic declines by slashing rates.[120] Post-Staggers, rail rates for all commodities fell by 55%, and correspondingly, the volume of intercity freight carried by rail, measured in ton-miles, doubled.[121] Railroads not only added volume but also recaptured a significant market share from competing modes. Recall, as noted in chapter 1, that by the end of the 1970s, rail's share of total intercity freight had fallen to a historic low 27%. By 2010, railroads had regained 43% of total intercity freight and were a viable competitor with other modes of transport.[122] Profitability followed reduced costs and increased traffic. Industry rate of return rebounded from the dismal low of an average level of 2% in the 1970s to above 9% during the second decade of the 21st century (see figure 2.3).[123]

Deregulation saved the rail industry. The new power to shed unprofitable track and set rates was a boon to industry and shippers: rates fell, volume and market share improved, and profits rose. In the aftermath of Staggers, U.S. railroads were, without a doubt, more efficient. The density of the U.S. rail system rapidly increased as more product moved across

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

a smaller network, and costs of service decreased.[124] Recent evaluations of the impact of deregulation have tabulated the annual savings directly attributable to regulatory reform to be between $7 and $10 billion, far in excess of even the most optimistic predictions.[125]

The Costs of an Efficient Rail Network

The triumphs of deregulation, however, came at a price. Rail companies have far greater power now as a result of the dismantling of the regulatory quid pro quo. The gutting of political controls leaves aggrieved publics with fewer avenues to hold rail companies accountable (a development only partially offset by the rise in other forms of shipping). Regulatory reform embraced the market and, in doing so, shifted power decisively toward private power—favoring large rail companies and large commercial customers. This social reordering was paired with material changes. Deregulation, as in other infrastructure sectors, improved the efficiency of the rail network at the expense of creating new (or enlarging existing) vulnerabilities. Just as postal reorganization created a more efficient network, the deregulation of rail emboldened railroads to optimize rail operations and the network. As part of the general improvement of market share and volume gains, deregulation supported increasing rail shipments of hazardous materials—a key flash point in post-9/11 debates about infrastructure security (see chapter 5)—and fostered intermodal substitution from small hauls traveling via trucks to large bulk rail shipments (a reverse of the substitution that had happened under regulation). Additionally, regulatory reforms hastened a reduction of the scale of underused, unprofitable track. The pruning of the rail network helped reduce costs and make the rail network a more efficient system of pathways and interconnections. However, by eliminating thousands of miles of track, rail shipments of dangerous materials now find it increasingly difficult to travel paths that are not in close proximity to dense population centers. These shifts eroded the observed security benefits associated with regulation.

Railroads' post-Staggers recovery of general freight volume and market share is matched by the increasing volume and share of hazardous materials shipments.[126] Post-Staggers, the total volume of hazardous materials transported by rail doubled, just as total freight transported by rail also doubled during the same period.[127] By 2012 rail and truck transported a nearly equal share of intercity hazardous materials, with rail carrying 27.6% and truck carrying 31.4% of the total ton-miles.[128] Significantly, rail rebounded to carry a significant share of the most dangerous commodity type: those that would later be the focus of the most intensive

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

security interventions, poisonous liquids and compressed gases labeled as toxic inhalation hazard (TIH) substances (see chapter 5). Looking closer at specific commodity type, in 2012 rail carried 65.9% of toxic poisons (Class 6 hazardous materials) and 37% of gases (Class 2 hazardous materials), while trucks transported 18% of toxic poisons and 41.3% of gases.[129] The figures were all record or near-record highs for rail and record lows for trucking since the tabulation of hazardous material data began in the 1990s. Cost is not the only factor determining shipping decisions, but deregulation plainly helped to shift hazardous materials shipments back to rail, just as it did for commodities more broadly.

The shift from truck to rail changed the dangers associated with the transportation of hazardous goods. A number of key factors define the risk of transporting such materials. The frequency of disruption (accident or intentional release), the size of the shipment, the toxicity or volatility of a substance, and the population density in the area of a potential release all shape the risk.[130] The characteristics of hazardous materials shipments differ in important respects between rail and truck. Rail shipments of hazardous materials are grouped into much larger bulk shipments and travel greater distances, while trucks transport small quantities for comparatively short distances. The average rail shipment of hazardous materials weighs 87.81 tons and travels 808 miles, compared to 4.82 tons and an average of 56 miles for shipments via truck.[131] Accident rates involving rail shipments of hazardous materials are significantly lower than for truck.[132] But the consequences of a rail accident are far more consequential. A single accident of an average rail shipment of TIH materials is an order of magnitude more severe in terms of loss of life and injury than a single average truck shipment due to the differences of shipment size.[133] On average, 10 times as many individuals are exposed, injured, and killed during a rail accident involving hazardous materials than during a trucking accident.[134] Outliers, extreme cases involving rail shipments, further skew the scale of the risk involved with rail transportation. Rail shipments of large quantities of TIH substances, and hazardous materials more generally, are a low-probability, high-consequence event. Though rare, a single accident involving rail shipment can result in catastrophic consequences.[135] For example, as a much-publicized report from Dr. Jay Boris of the Naval Research Laboratory noted, a release of TIH materials from a rail shipment in a densely populated area under ideal weather conditions could result in 100,000 fatalities.[136] In a sense, the danger of transporting TIH and other hazardous materials via rail is understated—dramatically so—by the historical record due to the relative infrequency of a serious

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

disruption under ideal dispersion and exposure conditions. Accidents involving trucks carrying hazardous materials occur more often, but they are, on average, localized and small-scale. Shipments via rail exhibit the opposite characteristics—they are infrequent and potentially catastrophic.

The derailment of railcars transporting chlorine in Graniteville, South Carolina, provides a glimpse into the possible scale of a major accident involving TIH materials. In January 2005 an accident involving railcars carrying chlorine led to nine deaths, the hospitalization of over 500 residents, and the displacement of over 5,000 people living near the site. The total costs from the accident were estimated at $126 million.[137] The accident could have been much worse. The derailment occurred during the middle of the night near a small town. A similar accident near a large city could have been catastrophic.

Here, the hidden or obscured costs of deregulation can start to be seen. The changes ushered in through deregulation have, for the most part, delivered a host of benefits for shippers and railroads. Yet the improved efficiency of the rail network has come with a price. The revitalization of rail service has led to a surge in rail shipments of dangerous materials. The move toward larger shipments via rail reduces the likelihood of frequent small-scale incidents but increases the long-term possibility of a catastrophic event. Additionally, the slashing of excess track across the network undercuts the added security afforded by an expansive rail network. A lean network that increasingly runs between heavily trafficked points and dense population centers limits the alternative routing options available to shipments of dangerous materials.[138] Under these conditions, skirting densely packed population centers—that is, utilizing circuitous routes that eschew the most efficient paths in favor of routes with comparatively low population densities—is made more difficult due to the elimination of redundant and inefficient track.

The Deregulation of Electric Power: Tight Coupling and Complexity

In the postal system and the railroad, industry sought deregulation as a way of getting out from underneath what they eventually came to view as burdensome regulations. Postal management viewed the system of congressional control over rates and budget as a noose around its neck that choked innovation; in rail, regulations that long benefited the industry became a millstone as trucking skimmed high-value shipping and cut deep into rail profits. In electric power, the dynamics were different. As in the other sectors, a mix of micro- and macrolevel changes undermined the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

seemingly stable regulatory compact that was in place and created new possibilities for change. But in electric power, it was the players sitting at the margins of the regulated system of vertical monopolies—known as qualifying facilities—that initially wanted to dismantle the regulated system. Their reasoning was simple: they wanted in.

As in both the postal system and rail, deregulation would substantially redraw the social *and* material outlines of the network. Competition would weaken core price-and-entry regulations. It would give private companies greater power to shape the market outside of close public supervision. Deregulation would also create new forms of systemic vulnerability. The partial deregulation of electric power remade the resilient network of networks into an increasingly fragile system open to large-scale failures. Under regulation, electric power developed as a system of (mostly) privately owned utilities operating vertical monopolies (combining all three phases of electric power: generation, transmission, and distribution) serving a limited territory. Regulation supported resilience by encouraging distributed control—each local utility maintained control for only one small corner of the larger interconnected power grid—and underwriting the development and use of specialized ICTs. Restructuring, however, undid these supports. It encouraged the centralization of control and the transformation of the use of ICTs in favor of standardized and accessible systems. Both of these shifts made the interconnected electric power system more susceptible to large-scale failures. As in the cases of post and rail, economic restructuring carries an often overlooked price: vulnerability.

The Road to Regulatory Reform: Unwinding the Postwar Status Quo

Between World War II and the late 1960s, the regulated system of electric power worked remarkably well. The Public Utility Holding Company Act (PUHCA) of 1935 and state regulation provided privately owned utilities, investor-owned utilities (IOUs), with monopoly protection and a guaranteed rate of return while imposing basic limits to protect the public from the volatility endemic to the holding-company scandals of the 1920s and 1930s, to deliver reasonable rates, and to expand reliable service. A broad consensus between the public, utilities, and regulators supported the status quo—what historian Richard Hirsh refers to as the *utility consensus*—for decades.[139] Under this consensus, utilities flourished, power consumption increased, and rates fell as new technological advances led to decreasing production costs. As with other infrastructures, regulations, once in place, obtained an inertia that made them difficult to dislodge.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Under regulation, utilities pursued what is described as the *grow-and-build strategy* of promoting increased consumption and lower costs through technological improvements.[140] Utilities invested in new large generators and increased thermal efficiencies to lower unit costs.[141] It worked. In 1960 the same amount of fuel could produce 50% more energy than it had during the 1940s.[142] At the same time, utilities lowered unit costs by investing in larger fossil fuel generators.[143] Thanks to these advances, as well as improvements in transmission and distribution, productivity increased by 5.5% per year between 1889 and 1963, outpacing all other sectors of the economy.[144] New efficiencies translated into precipitously declining consumer prices: residential prices fell from (adjusted) $4.53 per kWh at the start of the 20th century, to $.62 in 1927, $.47 in 1937, $.22 in 1947, and .$09 in 1969.[145] Utilities further promoted consumption and demand (and increasing capacity) through declining block rates that fell with increasing consumption.[146] The more you used, the less you were charged. Unsurprisingly, demand jumped as prices continued to fall, increasing by 12% annually between 1900 and 1920 and 7% annually between 1920 and 1973.[147]

Under the grow-and-build model, both consumers and utilities were satisfied and saw little reason to revisit the basic terms of service. Regulators, for their part, saw little need to be more than passive observers of utility behavior as long as industry and consumers found few points of contention.[148] Indeed, a mass of support developed around the utility consensus that made revision both difficult and largely unthinkable. The utilities and the public both received tangible benefits under the devised system, while ancillary interests, including manufacturers of electrical appliances; hardware manufacturers that supplied utilities with equipment; investors; and regulators, also supported the status quo.[149] In a familiar pattern, regulation appeared insulated from change. After the tumult and upheavals of the early decades of electrical power that had pitted consumers, industry, and government into increasingly confrontational configurations, the utility consensus provided a seemingly stable respite.

Cracks in the Consensus: Technological Stasis, the Oil Crisis, and the Emergence of Environmentalism

This seemingly stable system started to crack during the late 1960s and early 1970s as technological improvements appeared to reach their limits, the 1973 oil crisis rocked energy markets, and the newly sprouted environmental movement challenged escalating power consumption.[150] These developments undermined the foundations upon which support for the grow-and-build strategy rested and led to the cautious introduction of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

new competition into the field of electric power generation with the passage of the Public Utility Regulatory Policies Act of 1978 (PURPA).

By the late 1960s and early 1970s, steady improvements in thermal efficiencies and generating-unit size appeared to hit their limits and started to provide diminishing returns.[151] Utility managers could no longer rely on improving equipment to boost productivity. Technical limitations could not have arrived at a less opportune time for utilities. The 1973 energy crisis upturned energy markets globally and hit the U.S. electricity market hard.[152] U.S. utilities had increasingly adopted petroleum as a fuel source after 1960, increasing the total share of petroleum generation from 6.9% in 1962 to 20% in 1973.[153] During the crisis, the price of oil leaped from $1.77 per barrel to $12 and led to widespread inflation and stagnation across the economy (what came to be known as *stagflation*).[154] The rising price of oil inflated electricity rates: residential rates (in unadjusted terms) increased from $.021 per kWh in 1969 to $.044 a decade later (industrial prices, likewise, increased from .$009 to .$026 per kWh over the same period). The energy crisis, in an unprecedented development, led to what was then an unthinkably paltry increase in consumption: electric power use increased by *only* .1% from 1973 to 1974 and a very modest 1.9% the following year.[155]

Against these micro- and macro-changes, the emergence of the environmental movement in the 1960s and increased activism in the 1970s rose to challenge the promotion of continued growth of power consumption. The Clean Air Act (1963), the National Environmental Policy Act (1970), and the creation of the U.S. Environmental Protection Agency (1970) reflected the growing awareness of environmental issues and the increasing influence of organized activists (as did the celebration of the first Earth Day on April 22, 1970).[156] The National Environmental Policy Act, subsequently amended in 1974 and 1977, provided public agencies with the power to review and make public the environmental impacts of new projects—opening the door for increased activism and legal challenge.[157] In the realm of electric power, regulatory review of utility projects now became contentious. Opponents both from the environmental movement and the consumer movement started to aggressively confront and counter utilities.[158] Through the 1970s, activists successfully challenged the grow-and-build model and introduced principles of conservation and demand management (limiting consumption) into utility planning.[159]

Together, technical stasis, the oil crisis, and increasing activism challenged the calcified structure of electric power and created new openings for incremental change. The grow-and-build strategy found support

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and generated positive feedback as long as technological improvement supported increasing returns, cheap raw materials remained available, and environmental impacts were overlooked. However, once these basic conditions shifted, change, even if only seemingly marginal, became an option. It was no longer possible, or perhaps even desirable, to continue the status quo. President Carter attempted the ambitious task of redrafting energy policy through an expansive and detailed National Energy Plan, introduced in 1977, in an effort to reduce reliance on foreign oil and mitigate harmful environmental effects.[160] Carter's sweeping plan would be divided into different bills and picked apart in fractious debate. But, eventually, a watered-downed version would pass into law.[161] One little-remarked on aspect of this larger plan that was lost amid the larger debates, Section 210 of PURPA, would prove transformative. It began to introduce new competition into electric power and set the stage for more thoroughgoing and unexpected deregulation.[162]

PURPA and the Rise of Independent Power Generation

Section 210 of PURPA intended to stimulate nontraditional, non-utility forms of power in order to reduce dependence on foreign oil imports and lessen environmental damage. Section 210 created a guaranteed market for power from cogeneration facilities—facilities that transform what would otherwise be wasted heat into electricity—and renewable sources by forcing utilities to purchase power from qualifying facilities (QFs) at the avoided cost at which the purchasing utility would have spent to generate energy.[163] Before PURPA, regulated utilities were not only the exclusive suppliers of electricity to the public through transmission and distribution facilities but were also the sole market for power produced by cogeneration facilities.[164] Taking advantage of their unique position, utilities had little reason to offer cogeneration facilities decent rates or open their network to outside suppliers.[165] Section 210 of PURPA sought to remove these barriers and open utilities to outside supply. At the time, incumbents saw this provision as trivial. Section 210 was working at the margins of industry—non-utility sources amounted to less than 4% of total capacity in 1978—but it would in time prove revolutionary.[166]

Section 210 created a new category of power producers, QFs, and it carved out for them a guaranteed market on generous terms. PURPA exempted QFs from the PUHCA and state laws regulating rates, and it did not require them to register as utilities.[167] Critically, Section 210 specified that in tabulating avoided costs—a key figure in determining the prices utilities would pay to QFs—incremental costs rather than the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

lower marginal costs of production were to be used. The Federal Energy Regulatory Commission (FERC) went on to interpret Section 210 in the most generous manner possible for QFs. FERC specified that avoided cost would be calculated by using fuel and capital costs of plants built *after* 1978 in setting rates to be paid to QFs. These costs would be higher than the alternative pre-1978 costs. FERC's decision led utilities to pay high prices to QFs.[168]

PURPA opened up, for the first time, the vertical monopolies that had dominated electric power for the better part of a century. By legislative fiat it removed barriers to entry and created a robust market for non-utility power that aided the growth of independent power producers. As states implemented the law with FERC guidance, the total non-utility electricity delivered to utilities increased dramatically, from 6.034 billion kWh in 1979 to 28.03 billion in 1985 and 116.538 billion in 1990, moving from 3.5% of installed capacity to 5.5% in 1990.[169] By 1990, 7% of all electricity generated in the U.S. came from non-utilities, up from 2.9% in 1979.[170] PURPA, however, was only the first step in a broader push toward the deregulation and transformation of electric power.

The Energy Policy Act of 1992: Opening Electric Power to Competition

PURPA set in motion forces that would push comprehensive deregulation in the form of the Energy Policy Act of 1992. The success of small generators under PURPA discredited the notion that electricity was in all aspects a natural monopoly best served by a single integrated provider. This had been one of the key justifications for regulation since Insull's days. Importantly, the growth of independent power producers created a new interest group—QFs—that would advocate for the relaxation of regulations and the move toward wholesale and retail electricity markets. Further, the disparity between the prices offered by regulated utilities and QFs tempted large customers with the promise—or at least the possibility—that deregulation would lead to lower prices. This induced them to join independent producers in lobbying for deregulation. It was this ad hoc coalition of independent power producers and large industrial consumers that would be instrumental in pushing for deregulation.

Under PURPA, independent power producers took the lead in developing and implementing new small-scale, efficient gas turbines and other innovative technologies. Cogeneration plants by the 1990s could beat utility prices by 5 to 15%.[171] Free market economists had for decades attacked economic regulation in general and the regulation of electric power in particular as wasteful. The success of PURPA served as a tangible

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

example that they could now highlight. Unregulated power, so it seemed, could work just as well, if not better, than regulated utilities.[172] Insull's vision for the industry—vertical monopolies dotting the landscape—had grown hand-in-hand with state regulation. This model of organizing the industry was now starting to be dismantled.

While PURPA created a real-world laboratory to test the viability of competitive power generation, it also created a new, motivated constituency: independent power producers. The growth of QFs during the 1980s created a politically motivated interest group that, once established, pushed to solidify and extend their position. PURPA, by introducing independent power producers into the formerly staid world of utilities, in the words of Richard Hirsh, "altered the demographics of power within the utility system."[173] As in the case of the postal system and freight rail, deregulation was more than mere policy reform: it was a significant reordering of the social relations that defined key infrastructure players. Independent power producers lobbied hard for deregulation over the objections of entrenched members of the utility industry, which feared challenges to their position, in order to expand market access and reduce limits on operations.[174] Under PURPA, independent power producers sold power directly to utilities through agreements undertaken on terms defined by Section 210 (and state laws implementing the section).[175] As QFs grew in stature, they wanted greater access to markets and, by extension, the electric power grid. They also wanted a relaxation of the limits on size and fuel use to which non-cogeneration QFs were subject (these limits were in keeping with the spirit of PURPA to support alternative forms of energy and small-scale production).[176] Utility control over transmission and distribution networks limited QFs' access to larger markets. QFs could not easily sell power to end consumers or to other remote utilities as long as utilities maintained exclusive control over their transmission networks, which linked to other utilities through the electric power grid and distribution networks that connected end users. Size limits, more obviously, limited the scale of commercial QFs and presented a barrier to growth.[177]

Large industrial consumers joined independent power producers in pursuing the introduction of wholesale and retail competition. As occurred in other industries, such as rail, the introduction of partial competition at the margins created new inducements for players to advocate further deregulation. What began as small cracks in the status quo in time turned into seismic faults. The success of QFs under PURPA tempted large consumers of power to push for competition as a way of gaining access to cheaper supplies of power. Under the partial liberalization afforded by

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

PURPA, QFs in some states began producing power at costs lower than the retail prices offered by utilities (which were based on averaged costs and reflected historic investments). In certain markets a wide disparity opened between wholesale and retail prices. In areas with high retail rates, such as California and the Northeast, a gap of three to four cents emerged between retail and wholesale prices.[178] Large consumers, represented through the Electricity Consumers Resource Council (ELCON), lobbied for wholesale and retail competition in order to capture lower prices and, in effect, opt out of the regulated electric power market.[179]

The advocacy of independent power producers and ELCON found a favorable hearing within President George H. Bush's administration. The Energy Policy Act of 1992 embodied most, though not all, of their wishes. The act opened the power grid, the loosely interconnected network of networks that stitched together different utilities, by mandating wholesale competition among power generators, and it created a new category of power producer, *exempt wholesale generators* (EWG).[180] Though the precise rules governing such competition would be formalized by FERC in time, the law transformed the power grid into a marketplace. Now, utilities had to open their transmission networks to independent producers, allowing generators to sell power to different utilities and service companies (a process called *wheeling*). The Energy Policy Act in effect broke up the old utility system of vertical monopolies by opening generation fully to competition: no longer would a single utility control generation, transmission, and distribution. Through competitive wholesale wheeling, power could be sold across the grid and supplied to different end providers. The law, however, did not mandate retail competition but allowed each state to decide the retail question on a state-by-state basis.[181] The creation of EWGs represented an enlargement of the QFs established under PURPA. Unlike the QFs under PURPA, EWGs were not bound by efficiency requirements or subject to PUHCA regulations. EWGs, for example, did not have to abide by PUHCA restrictions on the use of debt and could be owned by utilities outside of their franchise area.[182]

In the years following the Energy Policy Act of 1992, independent power generation (QFs, EWGs, and other forms of non-utility power) grew rapidly as competitive wholesale markets replaced the staid utility model. Non-utility power accounted for 7.5% of total power generated (229,676.33 GWh) in 1990, 10.70% (358,958.77 GWh) in 1995, 20.69% (786,721.67 GWh) in 2000, 38.97% (1,580,577.19 GWh) in 2005, 40.08% (1,653,427.80 GWh) in 2010, 43.22% in 2015 (1,762,278.35 GWh), and 43.63% in 2017 (1,759,991.24 GWh; see figure 2.4).[183]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Additionally, a thriving wholesale market for power developed through which utilities, independent generators, and third-party power marketers sold electricity. In 2001, for the first time, the resale power market—electricity resold to a distributing entity or power-marketing company—outstripped total power generated: 3,736,643.65 GWh were generated while 7,345,319 GWh were sold on the resale market (see figure 2.5).[184] These power producers operate largely outside of the boundaries of

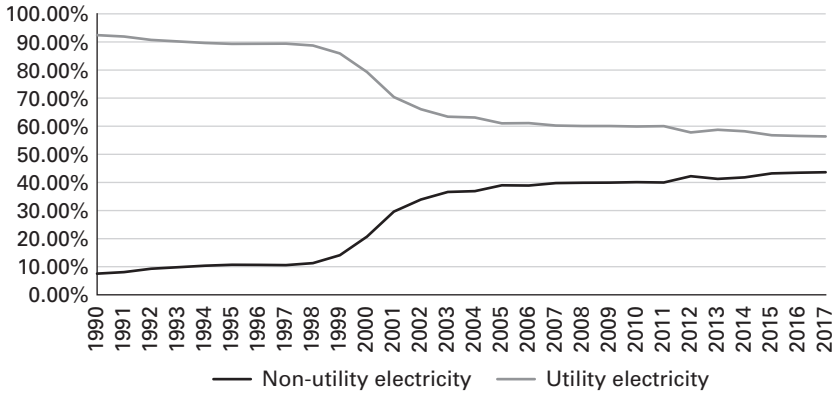


Figure 2.4
Percentage of utility and non-utility U.S. electricity generation, 1990–2017. EIA, "Electric Power Industry Overview: 2007"; EIA, "Net Generation by State."

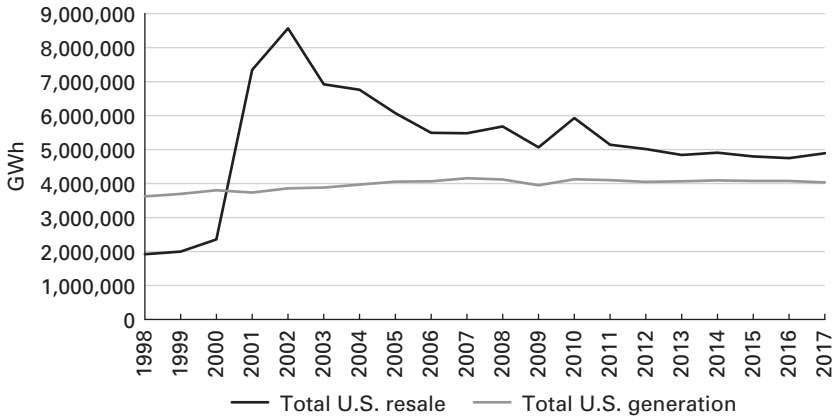


Figure 2.5
Total U.S. electricity generation and resale, 1998–2017. EIA, *Electric Power Annual 2009*, 53, table 6.2; EIA, *Annual Energy Review*; EIA, *Monthly Energy Review*, table 7.2a; EIA, "Net Generation by State."

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

traditional regulatory supervision—exempt from the bedrock state and federal regulations concerning rates and operating structure that have long supervised the industry.[185] State public utility commissions have been marginalized. As non-utility power has grown, public utility commissions have increasingly found themselves on the outside looking in.

Electricity Deregulation: Tight Coupling, Complexity, and New Vulnerabilities

Deregulation delivered social and material changes to electric power. It created new forms of competition that operated outside of the traditional boundaries of regulatory control and split open the vertical monopolies that had dominated electric power for decades. These new players—QFs, EWGs, power-marketing firms, and others—ran wild. The Enron scandal—which saw the company manipulate the wholesale electric power market—was just on the horizon. State and federal regulation had been a counterweight to the power of utilities, but now regulation appeared to have been traded for the market. Deregulation also transformed the interconnected electric power system in ways that enlarged or introduced new possibilities of failure. The push toward market liberalization was matched with consolidation and higher levels of centralized control. In order to create open-market access and coordination, new institutions, independent service operators (ISOs), and regional transmission organization (RTOs) now assume control over what were formerly multiple independent systems. The rise of centrally managed ISOs and RTOs supplants the balkanized network-of-network architecture previously supported by regulation (see chapter 1). More subtly, the dismantling of the utility system reorders the context within which firms operate and eliminates the incentives built into rate-of-return regulation to encourage long-term investment (even overinvestment) in new, expensive equipment in favor of bottom-line considerations. In tandem with restructuring, electric power companies increasingly turn away from isolated and customized control systems in favor of generative computing platforms and standardized commercial off-the-shelf (COTS) control systems. Both movements—the consolidation of individual systems into centrally managed constellations and the adoption of complex computing technologies—create new vulnerabilities and possibilities for large-scale failure that were previously discouraged under the old regulatory model.

Consolidated Control: ISOs, RTOs, and Organized Regional Markets

It was left to FERC to sort out exactly how deregulation would unfold. FERC Orders 888, 889, and 2000 set out the basic terms on which

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

competitive wholesale markets would replace the utility model.[186] In these orders, FERC attempted to eliminate the barriers that incumbent control of transmission networks pose to wholesale trading.[187] Instead, they encouraged the development of centrally managed markets. FERC requires utilities to functionally "unbundle" their networks by filing open-access transmission tariffs and offering nondiscriminatory access to transmission networks—that is, allow interested parties access to transmission services on terms comparable to that of the operating utility—and participate in an *open access same-time information system* (OASIS), linked through the Internet, offering all market participants up-to-date capacity and price data.[188] To satisfy these requirements, FERC Orders 888, 889, and 2000 strongly support, though do not mandate, the adoption of a regional, organized market structure overseen by ISOs and RTOs (henceforth, ISO/RTOs).[189] In organized markets, ISO/RTOs perform key functions: they host day-ahead and real-time spot wholesale markets; provide all participants open, nondiscriminatory access to transmission service and real-time information about grid conditions through the posting of system information and prices via OASIS; and, importantly, assume operational control of the transmission networks under their jurisdiction.[190] ISO/RTOs are subject to FERC supervision and operate independently from any market player.[191]

The ISO/RTO model has been widely adopted. ISO/RTOs now control the bulk of the U.S. electric power system (see Figure 2.6). By 2010, seven ISO/RTOs coordinated and controlled electric power service for the majority of the country, covering 35 states, including all of New England, the mid-Atlantic, the Midwest, and large swaths of the Southwest and California.[192] These seven ISO/RTOs now control power for 194 million customers—more than two-thirds of all electricity customers in the U.S.—and oversee 57% of total U.S. generation capacity.[193]

ISO/RTOs provide the centralized control and coordination needed to ensure that the interconnected electric power system remains stable. Under the ISO/RTO model, multiple independent local utilities voluntarily cede control of their transmission networks to the governing ISO/RTO to create a larger single control area—in effect, a much larger interdependent system (see figure 2.6).[194] ISO/RTOs assume operational authority over the accumulated transmission network and adopt many of the control functions that were previously the domain of individual utilities—most importantly, the critical functions of maintaining a real-time balance between supply and demand, forecasting, and dispatch.[195] Under regulation, system control was located at the level of the individual utility. Loose

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

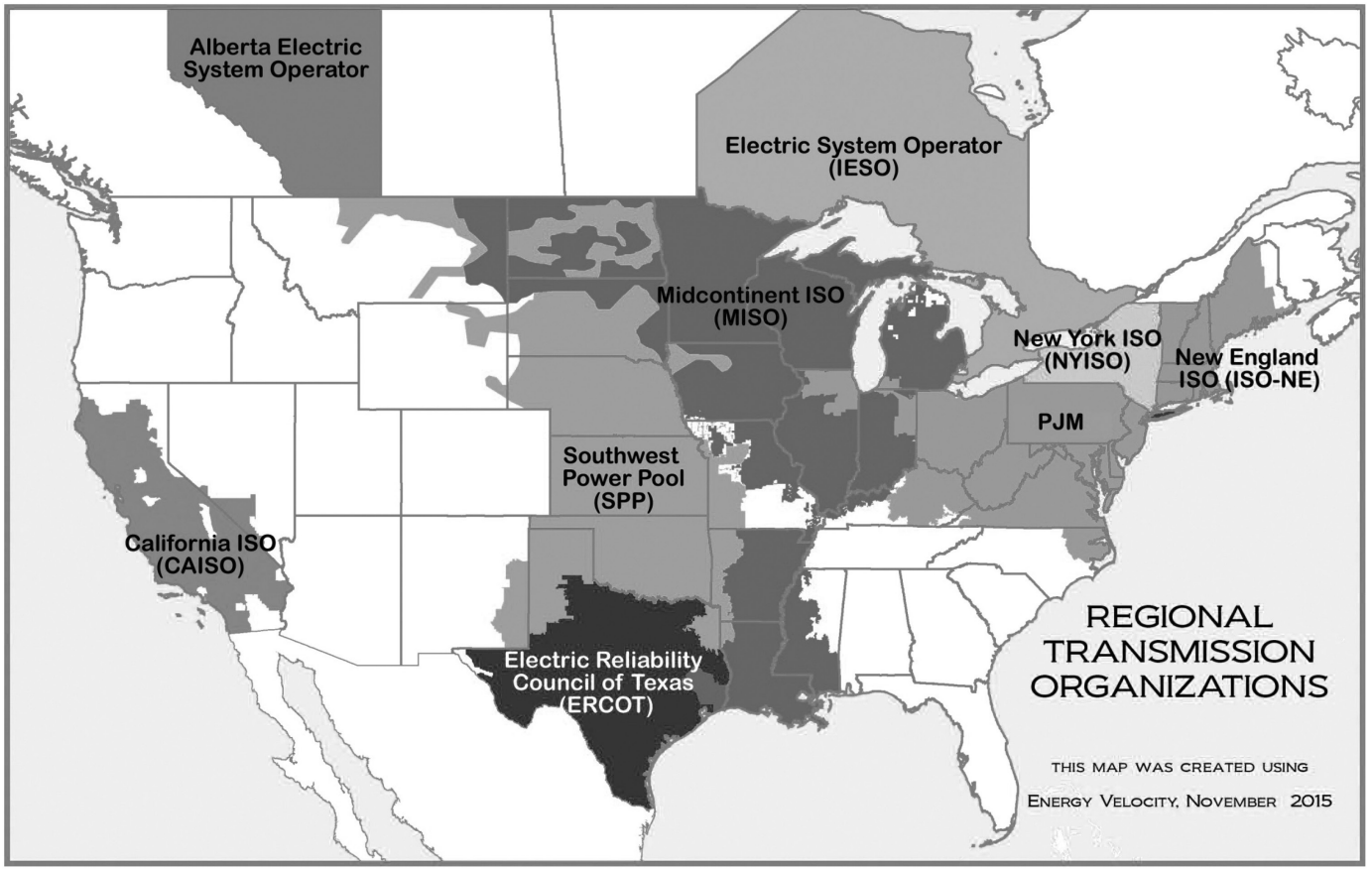


Figure 2.6
Regional transmission organizations, 2015. Image courtesy of the Federal Energy Regulatory Commission.

interconnection at the edges offered support when needed, but it allowed individual firms to retain a great deal of control—the promised "unity and autonomy" described in chapter 1.[196] Utilities relied on internal, intrafirm control and communication networks to maintain real-time monitoring, balance, and dispatch over integrated networks (combining generation, transmission, and distribution). Each utility oversaw its own fiefdom. Under deregulation, however, ISO/RTOs have taken responsibility for these functions. They have replaced intrafirm controls with centralized, interfirm controls located at the regional ISO/RTO level. Whereas under the utility model control was distributed widely and nested within each separate utility, ISO/RTOs aggregate control over many formerly distinct and relatively independent systems.[197] For example, the creation of the Electric Reliability Council of Texas (ERCOT) consolidated 10 separate control areas under its authority, while the Midcontinent ISO (previously known as the Midwest ISO) assumed control over 34 previously independent and separate transmission owners across the Midwest.[198]

The consolidation and centralization of control within electric power finds a close parallel with changes in the postal network. Recall that, in order to improve processing efficiency, USPS adopted new mechanization and, later, automated technologies and restructured the internal processing network around a limited number of large processing centers. The adoption of the managed ISO/RTO model follows the same logic: increasingly centralized control at higher levels is used to manage a large and growing network. In both the postal system and electric power, regulation undergirded distributed processing throughout the network. In order to capture new efficiencies under deregulation, however, loosely coupled network structures gave way to tight coupling.

The transformation of electric power aggregates risk in new ways. ISO/RTOs champion the apparent improved reliability they deliver.[199] ISO/RTOs note that consolidating and centralizing control over what were formerly multiple independent systems reduces the number of transactions and controllers involved in the provision of service. The ISO/RTO council, a collaborative comprising all operating ISO/RTOs with the exception of ERCOT, claims that "ISOs/RTOs enhance reliability through their large geographic scope—by dispatching generation over a broad region they reduce the number of decision makers managing the grid, which simplifies coordination and improves reliability."[200] Yet while consolidating and streamlining control may increase day-to-day reliability, it also increases the possibility of large-scale failure. Within the restructured network topology, ISO/RTOs stand out as dense hubs central to the operation of vast regional

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

interdependent power systems. Breakdowns in ISO/RTO control—due to operator errors, intentional attacks or sabotage, technological failures, or other causes—jeopardize the large interdependent electric power networks they manage. The balkanized structure of electric power under regulation militated against these possibilities by underwriting diverse centers of control. The enlargement of systems under a single authority—that is, moving from distributed to tightly coupled central control—erases some of these benefits. The failure of the New York Independent System Operator (NYISO), the California Independent System Operator (CAISO), or ERCOT, unlikely though it may be, undermines power not for a single community but for virtually an entire state, while the failure of larger ISO/RTOs threatens to destabilize service across multiple states. The new interdependences created by ISO/RTOs correspondingly increase the stakes of failure dramatically. In seeking the smooth functioning of competitive markets, the process of deregulation creates conditions sympathetic to large-scale failure.

Deregulation, Control Systems, and Complexity

Restructuring also more subtly helped transform how firms involved in the provision of electric power use ICTs. While the centralization of control areas under RTO/ISO supervision made electric power increasingly tightly coupled, shifts in technology added additional complexity into the mix. The injection of competition into the electric power market reordered the basic set of incentives under which firms operate and, in the process, set the stage for a shift in the type of ICTs electric power companies use. Power companies transitioned from specialized equipment dedicated to specific tasks that operated on isolated networks toward increasingly using generative multipurpose computers that run on public or multiuse communications networks.[201] These changes opened up the electric power system to malicious digital intrusions and new sorts of failures. Concerns about these sorts of failures would become pervasive after 2001. Rate-of-return regulation, as noted in chapter 1, encouraged firms to heavily invest in capital and adopt specialized ICTs (as well as other forms of new equipment) for operations management. Under competition, incentives shifted to maximize short-term efficiency and reduce costs. Firms facing competitive pressures replaced customized control systems operating on isolated communication networks with COTS systems compatible with common operating systems, such as Microsoft Windows, and linked them to the Internet or other multiuse networks.[202] In effect, specialized operational technology (OT) merged with a more conventional information technology environment.[203]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

These changes were significant: they shifted power companies *away* from linear computing technology in favor of increasing complexity. These changes impacted a number of different technological components and systems, including most significantly what are known as supervisory control and data acquisition (SCADA) systems. SCADA systems are computer-based control systems used to oversee and control remote processes in the provision of electric power (as well as other infrastructure sectors).[204] These systems are the outgrowth of control technologies developed and used during the middle decades of the 20th century. SCADA systems are the "digital brains" used in all phases of electric power—generation, transmission, and distribution—to monitor and control real-time distributed processes.[205] SCADA systems collect data from remote locations and send response commands based on programmed or operator controls from a control center to field devices, such as valves, breakers, capacitors, and transformers. Typical SCADA systems are made up of hardware and software components that include a master terminal unit (MTU) and human-machine interface (HMI), located at the control center; remote terminal units (RTUs) and/or programmable logic controllers (PLCs), located in the field; and communications links connecting the control center to field devices (see figure 2.7).[206] Historically, utilities invested in customized control equipment (hardware and software) designed for their specific operations. These systems, referred to as *legacy systems*, were designed for a single purpose, operated across isolated communication channels, and relied on specific and obscure communication protocols to exchange data.

In the 1990s, however, SCADA systems began to change. Changes in political economy reverberated in the technological mix used within electric power systems. SCADA systems shifted away from an ecology of single-purpose devices and dedicated equipment and became integrated with standard multipurpose—generative—computer operating systems. At the same time, new COTS equipment supports standard, routable communication protocols to share data and commands and piggybacks on accessible communication channels, such as the Internet and corporate intranets used for all sorts of corporate communications. Internal email messages and human resource reports in some instances now travel across the same networks as SCADA commands.[207]

These changes mirror larger shifts in computing and networking. As Johnathan Zittrain details in *The Future of the Internet—and How to Stop It*, beginning in the 1970s a dramatic shift occurred: dedicated computational devices and parochial networks were replaced by multipurpose computers, such as the Apple II, and the open, multipurpose network

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

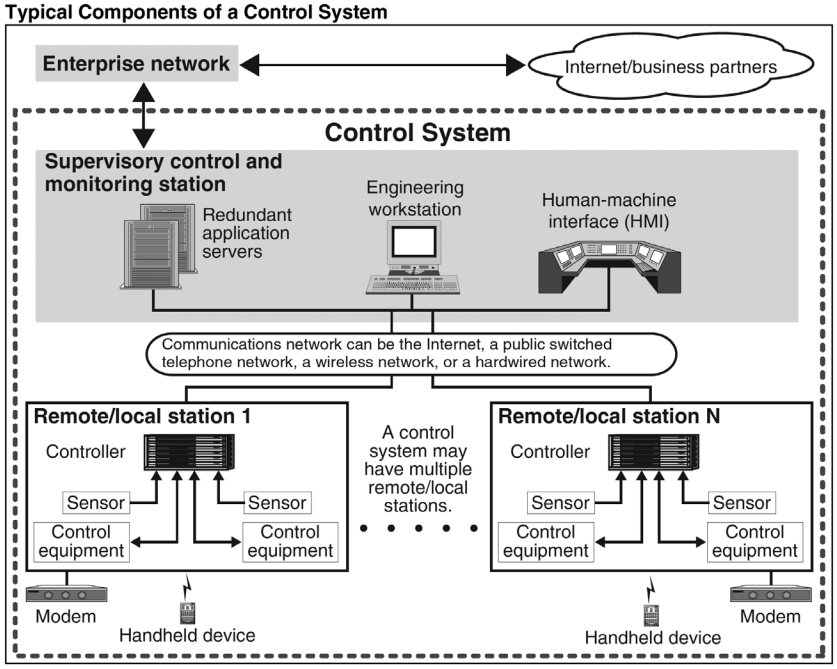


Figure 2.7
Typical components of a control system. Image courtesy of GAO, *Critical Infrastructure Protection: Challenges and Efforts*, GAO-04-354.

architecture of the Internet.[208] The restructuring of the electric power industry indirectly aided a similar transition or transformation in control system architecture. Deregulation transformed the basic model of utility operation and, just as importantly, investment. Rate-of-return regulation rewarded long-term, capital-intensive projects. Public utility commissions for decades were deferential to utility requests to undertake new projects. Indeed, increasing capital was one way to expand the rate base and hence returns.[209] The move to competitive markets, however, undercuts these supports. Under competitive markets, firms—including utilities operating competitive generation, independent generators, and third-party firms—are no longer rewarded by investing in new capital-intensive projects but rather for low costs and lean operations.[210] Without promised returns and in the face of competitive pressure, investment priorities shift toward low-cost opportunities and short-run profitability. In this context, support for expensive single-purpose control technologies evaporated, and firms began to adopt cheaper COTS systems and multipurpose networks.[211]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The new control-system architecture creates new opportunities for malicious exploitation and attack.[212] A successful cyber campaign can be divided into what Tim Mauer describes as four key phases: (1) *Planning and preparation*, collecting target reconnaissance and developing weaponized code to penetrate the target; (2) *cyber intrusion*, delivering the weaponized code to the target and exploiting an existing vulnerability in the target, (3) *persistent access and management*, installing malware on the target's system in order to allow remote command and control of the target; and (4) *execution of payload to achieve objective*, steal, destroy, or manipulate data, causing loss of access, information, or, in cases involving control systems, physical damage.[213] The shift in control-system technology makes each phase of an attack easier.

Esoteric and isolated control systems offered some measure of defense through obscurity. These features made phase one of a potential attack—target reconnaissance and the development of a way to exploit the system—difficult. Potential attackers have difficulty learning about these obscure technologies and uncovering vulnerabilities in these unfamiliar and unique systems. These systems are now far less mysterious. The increasing standardization of SCADA systems around a set of common communication protocols and vendor models makes testing and experimenting with these systems easier. They can now be bought relatively cheaply and probed for flaws with fairly simple equipment.

Phase two—cyber intrusion—has also been made easier. Previously, control technologies operated on isolated communication channels with obscure communication protocols. The shift to support TCP/IP and the use of multipurpose networks for communication makes these technologies easier to access. Merging SCADA operation with the Internet or other multipurpose networks, like a corporate intranet, creates new paths of entry for an enterprising intruder. Finding a way in is a precondition for any successful exploit or attack.

The integration with control systems and personal computers makes phase three—persistent access and control—and phase four—the execution of payload to achieve an objective—easier. The old single-purpose control technologies were not, in any real sense, generative. They could not easily be modified to run new programs. These systems were designed on contract by manufactures for specific purposes (and specific clients). Adding new functions—when possible—was cumbersome. The adoption of personal computers (PCs) into the control system architecture changed things. PCs are complex machines that can run software designed by others for different purposes. They provide a platform for various types of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

programs with relatively minimal restrictions. They are not designed for or limited to a narrow set of tasks or uses (in other words, they are *not* a linear technology).[214] This is the genius of the generative PC and the open operating system model—it supports programs created and designed by *anyone* for a range of different purposes. It allows for contributions from left field. Anyone who masters the basics of coding can write a program that runs on a PC. These features create rich opportunities for creativity and unexpected collaborations.[215] But this is also the PC's Achilles heel; its weakness as well as its strength. PCs can run malware—malicious code designed for nefarious purposes. They can be repurposed for both good and ill.[216] Integrating generativity into SCADA architecture makes it possible for malware to enter a system and also opens the system to hacking. Hackers can gain remote access to industrial systems, reprogramming or hijacking key processes and causing physical effects. Valves can be shut off, turbines can be sped up or slowed down, and emergency systems can be shut down. If SCADA systems are the digital brains of the electric power system, they can also be turned into Frankenstein's monster—hijacked to run amok against an operator's wishes.

Lowering the bar for each of these phases makes cyberattacks targeting control systems inside the electric power grid easier. Easier—but that's not to say *easy* or trivial. Causing an intended specific effect—the loss of power in a certain region, the failure of a particular piece of equipment—is still difficult.[217] It requires a good deal of detailed information about the system's engineering and the interaction between various components of the system (or luck).[218] But the changing control system environment lowers the bar for an attacker (and raises the stakes for defenders). Legacy systems were, of course, not perfect or immune to failure.[219] A well-trained insider could (and can) always cause significant damage. Yet the lack of accessibility and generativity created real barriers for intruders: to successfully penetrate a legacy control system, an attacker had to become well versed in fairly obscure communication protocols and system configurations. The perpetrator would have to successfully gain access to a communication network not easily accessible to nonauthorized users. Additionally, even if compromised these systems could not necessarily be reprogrammed or twisted to fit the whims of a perpetrator. Dedicated control technologies designed for specific customers—linear technologies—simply had a narrower set of affordances than their generative progeny.

The risks associated with control system vulnerabilities are not illusions. In 2003 the so-called Slammer Worm targeting the Microsoft SQL server found its way into FirstEnergy's Davis-Besse Nuclear Power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Station. The worm affected computer systems globally and spread to the Davis-Besse plant through unsecured connections between FirstEnergy's corporate network and the Internet. The worm disabled the plant's safety-monitoring system for nearly five hours, as workers scrambled to restore operation. Luckily, at the time of the incident the plant was idle. Here, the combination of standardized equipment and accessibility led to a potentially very serious system failure.[220]

A few years later, control-system security would make front-page news across the globe. In the summer and fall of 2010, reporters and security researchers uncovered a joint U.S. and Israeli cyber operation targeting the Iranian uranium enrichment facility in Natanz.[221] The worm—dubbed Stuxnet—took advantage of four previously unknown and undisclosed vulnerabilities in Windows to gain access to the Natanz industrial control system.[222] It reprogrammed the Siemens programmable logic controls (PLCs) at the facility.[223] It was able to speed up and slow down centrifuges seemingly at will with little detection, and confused facility operators could not see or understand what was happening.[224] This manipulation eventually destroyed a reported 20% of the centrifuges and dealt a setback to the Iranian nuclear effort.[225] The reporting was breathless. Here, it appeared, was the first, but surely not the last, volley of "cyberwar."[226] Code had been used to cause physical destruction through the manipulation of control systems components. By this point, researchers and policy-makers had been discussing the possibilities of such an attack for years. But now there was proof. The transformation of control systems created rich new targets for digital espionage and sabotage. With Stuxnet, the U.S. and Israel took advantage of this new environment to deal a blow to Iran. But the U.S. was not immune to the risks of this new world, either. Indeed, much of the first decade of the 21st century would be spent attempting to figure out exactly how to secure power systems in the U.S. from cyberattacks. Years of regulatory reform and technological change created a new set of vulnerabilities, and now it was time to determine how to patch and prevent them. As chapter 6 details, this would prove to be no easy task.

The Political Origins of Infrastructure Vulnerability

The political restructuring of price-and-entry controls reordered power within infrastructures and made them less publicly accountable. Price-and-entry regulations had been a long-standing way of building public values and representation into infrastructure operation. Flawed as these institutions were, they added a counterweight to the market power of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

key players and created venues where different entities could air their grievances. Under deregulation, certain market players were empowered as never before. Large-volume mailers, rail operators, key customers, and an entire fleet of new and transformed electric power companies were emboldened. Reform removed some of the key constraints that had limited the power of particular infrastructure publics over others. Deregulation took on an air of orthodoxy that regulation had previously assumed: it became a seemingly commonsense solution to a host of thorny and unique problems and contexts. During the late 1960s, it seemed quixotic to think that the postal system could ever be reformed. By the 1990s it seemed obvious that all infrastructures would and should operate according to the logic of the market.

These larger social and political alterations produced material changes within these networks. Deregulation created new contradictions within infrastructure services. It made infrastructures both more efficient *and* more vulnerable. It increased tight coupling and complexity within these systems. Reform led to the consolidation of physical controls at increasingly higher levels within both the postal system and electric power, creating new single points of failure and possibilities of cascading failure. It led to increasing bulk shipments of hazardous materials across a rail network maximized for efficiency, offering little incentive or option to route these dangerous shipments away from urban areas and increasing the chances of a catastrophic release. As a result of reform, power companies adopted increasingly accessible COTS equipment that controlled the physical processes of generating, transmitting, and distributing electricity, creating an environment ripe for malicious hacking. Seen in this light, the presumed successes of deregulation are qualified: efficiencies and (in some cases) lower prices are achieved at the price of greater vulnerability and brittleness. Likewise, from this angle the inefficacies of the old regulatory model, much decried during their day, appear to have offered some overlooked advantages. Regulation, for its myriad charged failings, built into infrastructures a degree of resilience. Stable monopoly or quasi-monopoly markets incidentally provided a check against systemic vulnerabilities and supported resilient configurations. Economic regulation, enacted for a host of other reasons, supported the creation and maintenance of systems characterized by loose coupling and linear organization. Despite appearing through the dimmed prism of economic efficiency to be wasteful indulgences, these qualities provided an easily ignored benefit: resilience. Deregulation undermined these benefits in the search for improved operation. In many ways, then, the new or enlarged vulnerabilities sketched

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

above represent not the failing of the project of regulatory restructuring but rather its *success*: the successful adoption of new efficient processes caused new vulnerabilities to be created and enlarged.

Foregrounding the connection between political restructuring—the project of deregulation—and infrastructure vulnerability challenges certain basic assumptions about the roots of infrastructure vulnerability. Rather than seeing infrastructure vulnerability as alternately the product of years of not-so-benign neglect, the autonomous logic of technological or economic progress, or an inevitability of private ownership, focusing on the transformations associated with deregulation highlights that vulnerabilities are politically and historically marked: they spring in part from critical and specific political decisions linked to the upheavals in infrastructure governance that first began to stir during the 1970s.[227] Contemporary challenges or problems in part reflect then not inevitabilities but the particular consequences of the political project of deregulation. In numerous U.S. government publications, the assertion that 85% of the nation's critical infrastructures are privately owned is repeatedly invoked as a way of explaining away vulnerability.[228] This is an important observation, but it only tells part of the story. The assertion elides the important role that regulation and public policy play in shaping and determining *how* private property is organized.[229]

The vulnerabilities sketched above, however, remained, for a time, largely obscured from view. Hidden in plain sight, the risks associated with centralized control, standardization, and the influx of shipments of hazardous materials across a greatly reduced network went (largely) unnoticed. For the most part, after deregulation the postal system, rail network, and electric power grid operated reliably; minor disruptions sporadically occurred and often occasioned little more than a raised eyebrow before returning to normal operating conditions. Yet while deregulation has not imperiled the reliability of day-to-day operations, it has created the conditions for rare and large-scale systemic failures. In the aftermath of the terrorist attacks of 9/11, the contradictions implicit within infrastructure restructuring would be pushed to the fore. No longer obscured, the overlooked costs of deregulation have been called to account, and the contradictions implicit within restructuring have become central objects of political debate and, ultimately, intervention. It is to this complicated process that the second half of the book now turns.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

II

Ubiquitous Targets: Infrastructure Security after September 11

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

3

Imagination Unbound: Risk, Politics, and Post-9/11 Anxiety

Life is good in America because things work.
—President's Commission on Critical Infrastructure Protection, 1997[1]

Infrastructures have *always* been dangerous. In the late 1870s, the Post Office Department's annual reports included a grim annex—a listing of casualties. Across several pages of small type, the Post Office Department's superintendent for Railway Mail Service provided accounts of the postal workers killed or maimed while transporting the mail by railroad. In 1878, General Superintendent of the Railway Mail Service (and future president of American Telephone & Telegraph [AT&T]) Theodore Vail offered a bleak introduction to the table of casualties:

> The following list of casualties will give some approximate idea of the continual risk to which the employés of this service were exposed; hardly a week passes but some employé is killed, oftentimes in the most horrible manner—maimed for life, which is worse—or so injured that for weeks and months he can perform no service.[2]

Vail recorded various train derailments, crashes, fires, and other accidents that affected both postal workers and the mail. He mixed accounts of bodily harm with descriptions of the impact of the accidents on the mail. The entry for September 21, 1878, is instructive:

> *September* 21.—New York, Central and Hudson River Railroad, Chicago express, collided with freight-train near Rome, N.Y. Both engines, mail, and baggage-cars completely wrecked. Head Clerk John S. Tunnard, and a fireman and brakeman killed, and Postal Clerks Frank O. Roberts, George W. Fitch, William E. Earle, and William H.S. Sweet Seriously injured as were many railroad employés and passengers.
>
> Some of the registered matter was badly mutilated, but no mail known to be lost.[3]

The postal system—and the rail system—of the late 19th century was dangerous. It was hazardous to both the workers who helped move the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

mail and the messages—letters and other postal ephemera—that flowed through the sinews of the system. Postal clerks often died, lost limbs, and faced other serious ailments in the course of their jobs. To them, the postal system was certainly a dangerous place. And, as Vail's account makes plain, postal managers were acutely aware of these risks. Vail was writing in part to advocate for pensions and other benefits for injured workers.[4]

The postal system, freight rail network, and electric power grid have—to some—always been dangerous. For centuries, local communities feared that mail could spread disease. At different points in time, letters were taken to be carriers of plague, cholera, yellow fever, and a host of other maladies.[5] These fears led to baroque practices of postal disinfection, including specialized fumigation devices, a complex array of markings certifying the "health" of the mail, envelopes specifically designed to allow for cleaning, and disinfection stations.[6] More blunt techniques were also used. During epidemics of yellow fever, shotgun-wielding bands of worried locals would refuse to allow railcars carrying mail that arrived from areas where the disease was present to stop and unload.[7] Railroads were also feared: rail accidents were spectacular and frequent occurrences for much of the first century of railroading.[8] These accidents were staples of mid- and late-19th century newspapers and subjects of popular concern.[9] Charles Dickens remarked on the horrors of American rail travel during his visit to the U.S.[10] For many, electricity remains worrisome: to a home filled with young children, electrical outlets remain an acute source of danger. A curious finger can result in an unwanted lesson in electrocution. "Toddler-proofing," the ritual transformation of an area into a place more suitable for kids, often includes placing cheap plastic covers over each outlet in order to lessen this risk.

In a sense, infrastructures *have always been dangerous*. Different publics relate to infrastructures in different ways. To some, these sociotechnical systems have always been imbued with hazard; to others, these systems are benign. Sometimes arguments about infrastructural risk are marginal—a minority opinion that is ignored. Other times, these ideas become powerful. They are adopted and translated into new policies, laws, technologies, and practices. They, in short, lead to infrastructural transformation.

* * * *

Part I of this book detailed how deregulation pushed infrastructures into newly vulnerable configurations. These material changes made new types of large-scale failure possible. But the identification and prioritization of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

these systems as public problems required a larger cultural context that would make claims about infrastructure insecurity legible; it required institutions that would legitimize, accept, and act on these claims; and it required a set of organizations that would argue and push for new forms of infrastructure protection and security as a goal. Material changes on their own are worth little. Many things are potentially dangerous—risk resides nearly everywhere you look. Making a particular source of risk salient, elevating *this particular problem* into something that captures the public imagination, and placing this risk over all of the others that compete for attention and attending is not automatic. It is a social process that is inseparably bound with the material world.

In this respect, post-9/11 changes were crucial. The terrorist attacks of 9/11 were a profound tragedy. Terrorism quickly moved to the center of both foreign and domestic affairs in the U.S. It became—and nearly two decades later largely remains—a dominate prism through which to view and evaluate domestic security and international law and policy.[11] In remarks on September 11, 2001, President George W. Bush declared that America and its allies would be united in a "war against terrorism."[12] This war—fought not against a single enemy or nation but a more sweeping and expansive confrontation with a form of political violence—would justify myriad legal and policy transformations in the coming years.

President Bush quickly prioritized infrastructure security and protection as key elements of a newly launched homeland security strategy after 9/11. The global war on terror became a powerful lens through which to interpret all manner of topics, including infrastructure. The government suddenly embraced and elevated ideas about infrastructure vulnerability that had circulated with little currency in the prior five decades. This prioritization of infrastructure security by the Bush administration legitimized the cultural framing of infrastructures as dangerous objects in need of taming. Now, arguments that took as their starting point the vulnerability of infrastructure and the possibility of terrorist attack made sense—they were culturally intelligible and seen as legitimate. This cultural shift was backed by a set of supporting institutional changes: billions of dollars would soon become available for infrastructure security at the federal and state level; a new department—the Department of Homeland Security—would have infrastructure protection and security as one of its key charges; at every level of government, "security" would soon become a familiar and accepted way of directing the thinking about infrastructure. Organized interest groups and newly formed political coalitions would adopt the language of security and the war on terror to argue

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

for infrastructure reforms. Now, a host of organizations could put forward claims about infrastructure security and find audiences and venues that accepted these arguments and, importantly, resources to address these concerns. The material changes that deregulation ushered in mattered: they created new possibilities of failure. But it was only thanks to the overlapping cultural, institutional, and organizational shifts and reorientations that occurred after 9/11, that these changes were transformed into public problems.

This book now turns to map how the postal system, freight rail network, electric power grid, and other infrastructures were reframed as "dangerous things" in the wake of 9/11 and considers how in the years that followed new security interventions remade the material and organizational foundations of these infrastructures. The previous chapters examined the upheavals and transformations of deregulation. Viewed through the lens of the unfolding war on terrorism, these changes are now reframed and reinterpreted as public problems. The long-presumed virtues of deregulation—lean and efficient networks unencumbered by "meddlesome" regulation—appear in this new light to be vices. In the long post-9/11 moment, the celebrated successes of decades of deregulation are thrown into serious question. Contemporary infrastructure security debates wrestle with an uncomfortable reality: deregulation created networks prone to large-scale failure and, at the same time, it largely delegitimized public accountability and stewardship over infrastructure in favor of the free hand of the market. As policymakers and a cross-section of civil society groups began to consider how to make infrastructures secure in the days and years after 9/11, deregulation implicitly and explicitly went on trial.

This chapter charts how *critical infrastructure protection* emerged as a key governmental concern in the months and years after 9/11. This shift—rooting infrastructure within the larger realm of geostrategic conflicts and discussions of national or homeland security—was not a given. Rather, it resulted from deliberate policy decisions made at the highest levels of government. This chapter provides a window into how critical infrastructure protection moved from being a little-discussed topic of concern, hidden safely in obscure government reports and the little-read musings of DC think tanks into a taken-for-granted way of thinking about infrastructure. This shift set the stage for the conflicts over infrastructure governance that were to come.

In order to sort through this reframing, the second half of the chapter dives into a theoretical discussion about the political possibilities—and limitations—of risk. The work of Ulrich Beck and others set up an

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

interesting debate: Can risks spark democratic engagement? Can they serve as the foundation for new forms of collective action that challenge the sunk politics buried within the organization of infrastructure? Or are risks, inevitably, an ally of the powerful—a cudgel used to blunt attempts to democratize infrastructure? The subsequent chapters of the book flesh out this theoretical discussion by examining how organized interests took advantage of the threat of terrorism to remake and refashion the postal system, freight rail network, and electric power system.

Ubiquitous Targets: Rethinking and Reframing Infrastructure

In the days that followed the terrorist attacks of September 11, infrastructure security became a key national priority. Infrastructures often hide in plain sight—when they work, most people almost never think about them. As long as the lights stay on, water flows from the tap, and our shipments from Amazon arrive (nearly) on time, most of us waste little thought on the complex web of systems that make the conveniences of day-to-day life possible. After 9/11, however, infrastructures became newly visible. Policy-makers were chastised for failing to prevent the atrocities of 9/11. The National Commission on Terrorist Attacks upon the United States ("the 9/11 Commission") memorably described the systematic failure of the U.S. government to prevent the attacks as "a failure of imagination."[13] In post-9/11 America, imagination was unbound. Policy-makers, operators, and the public began to see terror lurking *everywhere*: wastewater systems, bridges, shipments of hazardous materials, the electric power grid, and even the postal system appeared to be possible targets. Terrorism made the familiar appear sinister. Infrastructures—the dull and boring systems that comprise the background wiring of modern life—were quickly and anxiously foregrounded as sites of vulnerability and fear. They were transformed in the public imagination into "dangerous things" and pulled firmly into the ambit of national security.

The recasting of infrastructures was driven by the highest reaches of the federal government. President Bush quickly placed infrastructure protection at the center of his domestic security agenda. On October 8, Bush signed an executive order creating the Office of Homeland Security within the White House and establishing a new interagency Homeland Security Council.[14] On the same day, the president named former Pennsylvania governor Tom Ridge as the first director of the office.[15] In remarks made during Ridge's swearing in ceremony, Bush noted that infrastructure protection would be one of the core missions of the new office and that the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

office would seek to "strengthen and help protect our transportation systems, our food and water systems, and our *critical infrastructure* by making them less vulnerable to attack."[16] Pointedly, Bush framed infrastructure protection in expansive terms—arguing that the challenge of homeland security called for the protection of a range of disparate networks and systems that could be yoked together under the fuzzy rubric of *critical infrastructure*.[17] Rather than interpreting the terrorist attacks narrowly—focusing only on airline security, the infrastructure most directly relevant to the attack—the threat, in Bush's view, called for a larger rethinking of infrastructure. The executive order put the Office of Homeland Security in charge of coordinating efforts to protect infrastructure from the consequences of a terrorist attack.[18] It identified particular infrastructures for attention, highlighting transportation, energy, and telecommunications systems while also broadening the scope of what infrastructures would be included by adding the undefined term *critical infrastructure*.[19]

In late October, President Bush signed the USA PATRIOT Act of 2001 into law.[20] The law was sweeping, touching on surveillance reform, compensation for victims of terrorist attacks, and other areas or counterterrorism law.[21] It also defined critical infrastructure. Section 1016 of the act, known as the Critical Infrastructure Protection Act of 2001, defined critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[22] The law, however, provided little in the way of new authorities or funding for infrastructure protection: just a modest $20 million for the creation of a new infrastructure analysis center within the Defense Threat Reduction Agency.[23] The new law affirmed that the policy of the U.S. was to ensure that any and all disruptions to infrastructure be "brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States."[24] This language was important. It made it clear that infrastructures were now being viewed through the lens of security concerns (as a core part of an emerging definition of *homeland security*). Yet the Patriot Act and the executive order establishing the Office of Homeland Security said little about what, exactly, was to be done. How the U.S. would precisely go about securing the various transportation, power, telecommunication, and other networks that might be included in the category of critical infrastructure was very much an open question. What form these new security interventions would eventually take, their impact, and their

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

significance would be decided in the years to come through contentious and bitter negotiation and maneuvering. Infrastructure security was now, at least symbolically, a key front in the war on terror. The implications of this recasting, however, were still unknown.

The Cultural Construction of Infrastructure Vulnerability: A Partial History

The reframing of infrastructures as dangerous objects began immediately after the attacks of 9/11. But, this recasting rested on a deep foundation. Part I of the book charted the material and historical foundations of infrastructure vulnerability. Political and economic changes in how infrastructures are governed introduced new forms of vulnerabilities and new possibilities for failure. Yet this is only part of the story. These vulnerabilities and risks were not necessarily obvious. Risks never speak for themselves. That these risks, these vulnerabilities, and these systems—as opposed to others—would in time be identified and fashioned into public problems was not inevitable. On the contrary, it required a particular type of vision, a particular way of understanding and making sense of infrastructures, to transform these networks into topics of public concern. In this fashion, infrastructure risk was *coproduced*—it sat at the intersection of material and cultural change.[25] The cultural redefinition of infrastructures as dangerous objects did not appear out of thin air. In those early days after 9/11, Bush and the administration drew from and built on ideas and cultural constructions that had been gestating at the margins with little attention and little currency for decades. As Andrew Lakoff, Stephen Collier, and Eric Klinenberg have expertly mined, there is a rich genealogy beneath the contemporary rush to consider infrastructure as a national security problem.[26] Working during the Cold War and immediate post–Cold War period, policy-makers and defense thinkers began to articulate a set of concerns and a way of thinking about infrastructure that would come to dominate post-9/11 politics. In a series of little-read research reports and policy documents, these groups sketched out concerns over the increasing brittleness of civilian infrastructure, the impact that computerization might have on infrastructure vulnerability, and, most significantly, the ways in which terrorists might exploit infrastructures to cause significant economic disruption and, possibly, loss of life. Before 9/11 these ideas were marginal and received little traction (either inside the government or outside). After 9/11, they became ascendant. They offered a vocabulary for thinking about infrastructure that would

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

become commonplace. Although the various policy wonks, researchers, and government officials that fashioned these concepts in relative obscurity during the second half of the 20th century could not have realized it at the time, these ideas would provide the conceptual foundations for the most significant restructuring of the federal government since 1947.[27]

Infrastructure protection was a recurring, though decidedly minor, theme during the Cold War and immediate post–Cold War period.[28] Cold War civil defense efforts focused in part on strategies to protect infrastructure from military strike. In the 1950s and 1960s, a rotating cast of governmental bodies tackled the issue of infrastructure security. The National Security Resource Board (NSRB), the Federal Civil Defense Administration, the Business and Defense Services Administration, the Office of Defense Mobilization, and a host of other long-forgotten organizations sounded the alarm for infrastructure security.[29] As schoolchildren practiced duck-and-cover drills, these bodies focused on the brittleness of the U.S. energy, communication, manufacturing, and transportation systems in response to a military strike. U.S. Cold War strategy rested on three pillars: containment, deterrence, and preparedness.[30] Preparedness had its own grim logic: It suggested that a Soviet attack was all but inevitable. Therefore, key infrastructure systems should be made sustainable in order to survive a military attack.[31] A steady stream of governmental reports pointed out the challenges of infrastructure vulnerability—often with little noticeable impact. In the early 1960s, the Defense Electric Power Administration released a report on the vulnerability of the electric power system.[32] Reports by the Government Accounting Office (GAO) and the Congressional Research Service (CRS) during the late 1970s and early 1980s warned that the U.S. pipeline system and electric power system were both susceptible to attack.[33] The ambition of these efforts exceeded their grasp. For example, the National Security Resource Board led an effort of *industrial dispersal*—a plan to limit the concentration of industrial facilities in particular geographic regions.[34] Spreading out key industrial facilities, the thinking went, would make military strikes against the U.S. less devastating. But moving industrial facilities away from population centers or important resources proved nearly impossible. As the NSRB's own chairman, Arthur Hill, noted, it was entirely impractical to attempt to break up or relocate the production of steel outside of Pittsburgh.[35]

In the 1970s an important pivot occurred. Planners started to move beyond an exclusive Soviet focus and consider a range of possible threats targeting infrastructure. The terrorist attacks during the Munich Olympics led the Nixon administration to create the Cabinet Committee to Combat

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Terrorism and, subsequently, the Interagency Study Group to consider how to prevent and respond to international and domestic terrorism.[36] In the following years, the work of the study group looked beyond the boundaries of a Cold War confrontation and started to take seriously the possibility of a terrorist attack targeting transportation infrastructure, the electric power grid, or nuclear facilities.[37] It concluded that the risk of what it termed *intermediate terrorism*, attacks that did not rise to the level of mass destruction but were more consequential than a single abduction or assassination, deserved serious attention. A high-profile study conducted by the Center for Strategic and International Studies (CSIS) and cochaired by Robert H. Kupperman (the former head of the Interagency Study Group) and future CIA director R. James Woolsey attempted to push the topic of infrastructure security into the forefront of political conversation.[38] The report, *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*, was blunt and explicit.[39] America's networks were targets in waiting. CSIS stated that infrastructures represent the "fragile fabric of our nation" and wrote:[40]

> U.S. national security vulnerabilities do not lie solely in the Middle East, or Western Europe, or Central America, or the Western Pacific. Inside the United States itself, we have grown dependent economically, technologically, and psychologically upon highly complex service networks for our well-being. The telephone, electric power system, oil and gas pipelines, railroads, ocean and river shipping, and highways have become integral parts of our lives. We have come to take these networks for granted … yet, these domestic networks … suffer from procedural and technical vulnerabilities to serious accidental or deliberate disruption. … We cannot withdraw even in theory from the U.S. electric power grid, the computer and telecommunications systems, or our internal transportation networks.[41]

The CSIS group was direct: infrastructure vulnerability was a key national security challenge; the networks that the nation relied on were vital and brittle. The report, much like those that had preceded it, made little impact.

The most significant foundation for the post-9/11 rise of infrastructure security was the work completed by the President's Commission on Critical Infrastructure Protection (PCCIP) in the mid-1990s. The PCCIP could not have predicted that its work would have a fate in any way different from the various reports and warnings that had been produced, to little effect, in the previous decades. Timing, however, was everything.

In the wake of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, President Clinton signed Presidential Decision Directive 39 (PDD 39), "U.S. Policy on Counterterrorism."[42] The directive outlined U.S. counterterrorism policy and set the stage, indirectly, for the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

creation of the PCCIP. The first section of PDD 39 was titled "Reducing Our Vulnerabilities."[43] The directive instructed the Department of Justice (DOJ) to convene a cabinet-level interagency group "to review the vulnerability to terrorism of government facilities in the United States and critical national infrastructure and make recommendations."[44] The day-to-day work was led by Deputy Attorney General Jamie Gorelick.[45] The working group—dubbed the Critical Infrastructure Working Group—considered both terrorism and natural disasters.[46] The phrase *critical infrastructure* stuck. It would become a catchall term for conversations about national security or homeland security challenges relating to infrastructure vulnerability moving forward. In its final report, the working group identified eight critical infrastructure sectors—telecommunications, electrical power, gas and oil, banking and finance, transportation, water supply, emergency services, and continuation of government—and recommended that President Clinton establish a commission to comprehensively review infrastructure security and identify legal and policy options to mitigate these challenges.[47] It was an evergreen and classic inside-the-Beltway recommendation: when faced with a sprawling problem with no clear, easy answer, recommend a commission to study the problem further. Who could possibly object to more study?

President Clinton signed Executive Order No. 13010, "Critical Infrastructure Protection," in July 1996.[48] The order created the PCCIP and defined *critical infrastructure* as those national infrastructures that "are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[49] The language would be picked up in subsequent reports and eventually added with some alteration to the Patriot Act. The order adopted the eight sectors that the Critical Infrastructure Working Group had defined and tasked the PCCIP with consulting with key public and private sector stakeholders; assessing the scope of threats and vulnerabilities that confront critical infrastructure; identifying key legal and policy issues raised by the challenges of infrastructure security; and recommending a comprehensive national strategy to secure critical infrastructure. The PCCIP was chaired by Robert Marsh, a retired U.S. Air Force general, and featured commissioners from both the private sector (AT&T, Pacific Gas and Electric, IBM, Association of American Railroads) and government (Federal Emergency Management Agency, Department of the Treasury, Department of Defense, Department of Energy, DOJ, Department of Commerce, National Association of Regulatory Commissioners, Federal Reserve Board, National Security Agency, CIA, and FBI).[50]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The PCCIP worked for a little over a year and released its final report, *Critical Foundations: Protecting America's Infrastructures*, in the fall of 1997. At first glance the report echoes the conversations that had percolated within various corners of the government for decades: America's infrastructures are both vital to modern society and vulnerable to attack. More interestingly, the report roots its concern over infrastructure vulnerability in the context of a shifting, technological, political, and even economic landscape—what it calls "the new geography."[51] The prevailing tenor of the report is *anxiety*—over new technology, over the loss of the predictable (if terrifying) logic and stability of the Cold War, and over the perils of open markets. In this respect the report very much reads like the mid-1990s document it is. It spends a substantial amount of time describing the novel challenge of what it refers to as "cyber-threats." The commission argues that the diffusion of information and communications technologies creates new complexity within and across infrastructures and new forms of interdependency that could be exploited.[52] The commission is blunt: "We … face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications."[53] The commission also reflects on the post–Cold War security environment. Terrorism and crime and nonstate actors, rather than state-backed aggression, are the threats that receive attention.[54] Here, the PCCIP describes terrorism, financial crimes, and narcotics trafficking as the "dark side" of the new political, economic, and technological geography.[55] The report tentatively, and briefly, reckons with the economic and political foundations of infrastructure vulnerability. The commission acknowledges that deregulation made networks both more brittle and less accountable (it explicitly focuses on the regulatory changes in the energy, shipping, and telecommunications sectors).[56] Political restructuring, in its view, created efficient networks. But these changes carried a high price. The PCCIP writes that "today's processes are more efficient, but they lack the redundant characteristics that gave their predecessors more resilience."[57] That is, without the slack that used to be found within regulated infrastructures, even small attacks and disruptions can be amplified and have a significant impact.

In total, the commission painted a stark picture: the welding together of a global, just-in-time economy, defined by the ready movement of information, goods, and people, lowered the cost for terrorists and others to cause significant harm. The PCCIP offered modest recommendations—greater information sharing between the public and private sectors, the establishment of a new office of infrastructure assurance within the White House,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

an increase in education and awareness around infrastructure threats and vulnerabilities, and more.[58]

The PCCIP's report landed with a thud. Like the reports that preceded it, it largely went unnoticed. One of the commissioners, Mary Culnan, a Georgetown professor, joked that if the authors of the report wanted to get their picture taken with the president, they would "have to go down to the White House and get one of those big cardboard cut-outs [to] pose with."[59] Efforts to brief the president and vice president on the commission's findings were not successful.[60] Commissioner Bill Harris of the Association of American Railroads was equally tart, wryly remarking that "we were invited once to a larger meeting where the President was a hundred feet away from us. … That's as close as we ever got. We were never invited to the White House. … I didn't feel that anybody at the White House really cared about what we were doing."[61] The commission wanted a strong public statement from the president about the importance of the topic.[62] Months later, President Clinton did eventually reference the PCCIP's work somewhat indirectly during remarks at Annapolis.[63] To PCCIP chairman Marsh, this was not nearly good enough. As he remarked: "You would think that after eighteen months full-time effort … it would warrant … some strong statements out of the bully pulpit. But it didn't."[64]

Despite the cool reception, some internal changes were afoot. On May 22, President Clinton signed a new Presidential Decision Directive (PPD) that followed up on the PCCIP's work. PPD 63—"Protecting America's Critical Infrastructure"—envisioned the protection of infrastructure as a short-term challenge.[65] The PPD stated that by 2003 the U.S. would have the ability to protect critical infrastructures from intentional attacks that might affect government services, public health and safety, or the orderly functioning of the economy.[66] PPD 63 defined critical infrastructure as "those physical and cyber-based systems essential to the minimal operations of the economy and government."[67] In language that would be adopted nearly word-for-word in the Patriot Act in a few short years, PPD 63 stated that it was U.S. policy that "any interruptions or manipulations of [critical infrastructure] must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[68] PPD 63 moved with a light touch. Rather than pushing for the creation of new binding regulations on infrastructure operators, it supported voluntary cooperation between government and the private sector. It was explicit: critical infrastructure protection should be market-friendly. Close coordination between the public and private sectors is essential. After all, most infrastructures are owned and operated by

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the private sector. Yet the PPD was clear that government should "to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."[69] It went on to note that "incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection."[70] In cases in which market failure made some form of government intervention necessary, agencies should "identify and assess available alternatives to direct regulation," such as providing information for market participants and designing incentives.[71] The PPD called for the designation of a public-private National Infrastructure Assurance Council made up of private-sector infrastructure owners and operators and state and local officials. It placed a lead government agency in charge of each identified infrastructure and ordered the creation of the National Infrastructure Assurance Plan within 180 days. A new position within the White House, the national coordinator for Security, Infrastructure Protection, and Counter-Terrorism, was in charge of carrying out the new directive.

By the dawn of the presidency of George W. Bush, it looked like critical infrastructure protection would remain largely as it had throughout the Cold War and immediate post–Cold War period: a somewhat esoteric concern debated within a narrow circle of policy-makers and specialized researchers. By early 2001, the federal effort to protect critical infrastructure was led by the Critical Infrastructure Assurance Office—an obscure office hidden within the Department of Commerce's Export Administration with a modest annual budget of $5 million.[72] Total federal critical infrastructure spending fluctuated between $1.1 billion and $2.7 billion between 1998 and fiscal year 2001.[73] Before 9/11 the Bush administration had little appetite for investing in critical infrastructure protection, or homeland security, for that matter. A high-profile federal commission chartered in the late 1990s by Secretary of Defense William Cohen (and supported by President Clinton and Speaker Newt Gingrich) attempted to sound the alarm regarding terrorism and infrastructure vulnerability. Chaired by former Senators Gary Hart and Warren Rudman, the U.S. Commission on National Security/21st Century released its final report in February 2001, just days after the inauguration of President Bush.[74] The Hart-Rudman Commission conducted a detailed study of the post–Cold War national security environment. In one of its key recommendations, the Hart-Rudman Commission called for the creation of a new National Homeland Security Agency to oversee homeland security and, crucially, the protection of the nation's critical infrastructure.[75] In its view, infrastructure security was emerging to be one of the significant security

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

challenges of the 21st century, and the federal government did not have the capability in place to identify and address infrastructure vulnerabilities in a meaningful way. The Bush administration was skeptical of the idea of creating a new cabinet-level agency.[76] The Hart-Rudman report, like many others before it, was largely ignored. Chairman Rudman noted ruefully that the report went into the "dustbin at the White House."[77]

These scattered reports and commissions were attempts to invert infrastructure: to push to the foreground the systems that make up much of the background or our daily lives. In their own way, they each pleaded with policy-makers and, at times, the public to take note and look at the vulnerable foundations of contemporary life. They sought to plant infrastructures in the realm of security policy and view these systems through the lens of larger questions of geopolitics and conflict. By their own authors' ready admissions, these efforts largely failed. They rarely, if ever, sparked lasting or significant change. Yet threaded through these reports, documents, and marginalia is the creation of a way of understanding infrastructures that would later become powerful. Each of these reports and policy initiatives, in different ways, framed infrastructures as objects of anxiety and danger. They looked at different threats—a strike from the Soviets, terrorism, and other sources of possible attack and disruption. But they all agreed that the boring artifacts of modern life—electric power substations, wastewater plants, rail shipments, natural gas pipelines—were targets in waiting. They laid the groundwork for a cultural understanding of infrastructures as sites of danger in need of protection from external threats. The ideas charted through successive policy reports and mulled over for decades in the various odd corners of the federal government and aligned think tanks suddenly became in vogue in the post-9/11 context. After the terrorist attacks of 9/11, President Bush quickly adopted the vocabulary of the PCCIP: *critical infrastructure* found its way into speeches, executive action, legislation, and related press accounts with regularity. As President Bush pushed aside his earlier priorities and counterterrorism became central to U.S. policy, infrastructure security, or as it was now inevitably described, *critical infrastructure protection*, became a key pillar of this strategy. Moving forward, this conceptual framing and way of speaking and thinking about infrastructure would be taken for granted. The far-reaching and unanticipated consequences of this change would unfold in the coming years.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Institutionalizing Infrastructure Security: The Creation of the Department of Homeland Security

Infrastructure security became a top priority—at least symbolically—immediately after 9/11. But how *or if* this new prioritization would translate in practice was anybody's guess. During the first few months after 9/11, it was not at all clear if the repeated mentions by the administration of "critical infrastructure protection" were hollow or signaled the prospect of serious change. At first, it appeared that the Bush administration might balk at putting real muscle behind infrastructure security. The Patriot Act and the EO that established the Office of Homeland Security certainly borrowed concepts and ideas directly from the work of the PCCIP (and its predecessors). But the Patriot Act, as noted above, had only modest funding for new infrastructure security initiatives. While the Bush administration was quick to adopt the language and rhetoric of the PCCIP, how exactly it might approach the nuts and bolts of addressing infrastructure security was unclear. The PCCIP final report had pushed for the adoption of increased information sharing, a new White House office devoted to infrastructure security, and the creation of a private-sector council devoted to debating high-level issues. All of these modest recommendations had already been adopted in various forms by the late 1990s. The Hart-Rudman Commission outlined fairly grand ambitions. It called for the creation of a new cabinet-level homeland security agency tasked with infrastructure security as a key priority. The Bush administration resisted. It opposed creating a homeland security agency both before and in the months that followed 9/11.[78] In October 2001 Senator Joe Lieberman and Representative Mac Thornberry began to push a bipartisan plan to create a new "super agency" focused on homeland security.[79] Their plans would have merged a variety of agencies that had some homeland security responsibilities—something similar to what the Hart-Rudman Commission proposed—into a larger configuration. The White House rejected the idea. Throughout 2001 and into the late spring of 2002, the president and his aids repeatedly rejected the idea of creating a new homeland security agency. Instead, they supported the status quo.[80]

After beating back the idea of a new cabinet agency for months, in an about-face the president announced a proposal to create the new Department of Homeland Security during a televised address on June 6.[81] The reasons for the change in position are not entirely clear, but, as Mariano-Florentino Cuéllar argues, the decision to throw support behind a new agency likely reflected some mix of a recognition of the rising public

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and congressional enthusiasm for reorganization and a concern over the upcoming midterm elections.[82] The president's plan was even more ambitious than the previous congressional proposals. It included moving parts of over 20 agencies into the new department, including many functions and responsibilities, such as trade enforcement and agricultural regulation, that did not obviously fit within the definition of homeland security.[83] Under the president's proposal, the new department would have four directorates, including one devoted to information analysis and critical infrastructure protection.[84] After sustained haggling with Congress, President Bush signed the Homeland Security Act of 2002 into law on November 25, 2002.[85] In remarks that accompanied the signing of the bill, President Bush stated that "the new department will analyze threats, will guard our borders and airports, protect our *critical infrastructure*, and coordinate the response of our nation for future emergencies."[86] It was a massive reorganization. The new Department of Homeland Security (DHS) would contain roughly 170,000 employees and transfer all or part of 22 agencies to DHS.[87] The department followed, in broad strokes, the president's initial proposal.[88] DHS was organized around four directorates: Border and Transportation Security, Information Analysis and Infrastructure Protection, Science and Technology for Homeland Security, and Emergency Preparedness and Response.[89] The department's core mission focused on preventing terrorist attacks, reducing the United States' vulnerability to terrorism, and minimizing the consequences of terrorism.[90] The act created an undersecretary of Information Analysis and Infrastructure Protection (IAIP) to lead the new directorate and added two assistant secretary positions within the directorate—an assistant secretary for Information Analysis and an assistant secretary for Infrastructure Security.[91] The IAIP was tasked with assessing the vulnerabilities of critical infrastructure and reviewing threats and mitigations.[92] The directorate was also directed to produce a comprehensive infrastructure security plan and help prioritize efforts by state and local governments, other federal departments, and the private sector.[93]

Infrastructure protection took a prominent role in DHS and across the federal government. An institutional transformation was unfolding. Indeed, as homeland security funding started to flow, the commitment to critical infrastructure protection became clear. Federal support for critical infrastructure protection grew quickly. In 2003 the IAIP directorate was funded at $177 million; by 2004, its budget ballooned to $824 million.[94] This was a far cry from the $5 million budget that had previously propped up the Critical Infrastructure Assurance Office within the Department of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Commerce back in 2000–2001. Federal support for critical infrastructure security would only continue to spike in the coming years. Through various reorganizations of DHS, infrastructure security would remain a consistent priority.[95] By 2016, DHS was receiving $5.6 billion annually to fund its critical infrastructure work.[96] Total federal spending on critical infrastructure security likewise grew sizably, from just over $2 billion in 2001 to a stunning $20.7 billion in fiscal year 2016.[97] By 2016, federal funding devoted to critical infrastructure protection accounted for roughly 30% of *all federal homeland security funding* (which totaled a staggering $71.7 billion).[98] With the creation of DHS, infrastructure security was now—and would remain—an unambiguous key governmental priority. It sat as a key element of DHS's new mission and organizational design. The largest reorganization of the federal government in over five decades—since the creation of the Department of Defense—hinged in part on the prioritization of infrastructure security as an important governmental responsibility.[99] It was a stunning transformation. By 2016, over two dozen federal departments, agencies, and offices would report significant spending on critical infrastructure protection.[100] For decades, little-read reports produced by the bushel had been trying to nudge infrastructure security onto the top of policy-makers' agendas and into the public's consciousness, with little success. As one participant in the PCCIP noted, the phrase *critical infrastructure* had seemed "tailor-made to evoke yawns."[101] This marginal set of ideas moved to the center of policy discussions and now federal funding. It was both cemented in the culture and concretized within an expanding web of new institutions devoted to critical infrastructure protection. The idea that infrastructures were insecure spaces in need of protection from external threats—that these familiar systems should be viewed through the lens of larger geostrategic security concerns—firmly took root.

The Politics of Risk: The Radical Possibilities of a Promiscuous Resource

The rise of infrastructure security as a topic of significant public concern set the stage for new debates and conflicts over how infrastructures should be organized. Now, the context of even routine discussions and decisions about infrastructure operation—decisions about where to build a new high-voltage electric power line, policies concerning how a small municipal water system should operate, and many others—was colored by larger concerns about terrorism and security.[102] This shift in context

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

created a crisis of control.[103] There was no simple road map indicating how to integrate security protections into the day-to-day operations of expansive, multiuser, multiuse networks. This moment of crisis created a space to rethink and to remake how infrastructures would operate. Over the next decade and counting, infrastructures would become deeply contested spaces. The wisdom and impact of deregulation would be revisited and questioned. Infrastructure owners, workers, different sets of users, civil society groups, government regulators, and others fought (and in some instances continue to fight) bitterly to define the terms upon which infrastructure protection would rest. Before mapping how these disputes played out within the postal system, freight rail transportation, and electric power grid, it is useful to pause and consider the politics of risk. To understand how organized interests would marshal the threat of terrorism to transform infrastructures—how the fear of terrorism would be translated into durable sets of new infrastructural practices—it is useful to first take a detour and consider the political possibilities and limits of risk.

Novel risks are volatile political resources: they can scramble the status quo in surprising—even contradictory—ways. In some cases, risks can provide the foundation for new forms of democratic activity and political formations. They can split open previously closed domains to close scrutiny and support new forms of collective action; they can rip topics seen as outside of politics back into public view and consideration; and, at the same time, they can offer the scaffolding upon which new political coalitions are created. In certain circumstances risks can spark political reversals: they can support the democratization of spaces previously cut off from public participation and accountability and amplify the voices of marginalized groups. But these are only possibilities—and fragile possibilities at that. As the coming pages and chapters detail, the politics of risk are complex. Risks can also be twisted to serve illiberal purposes, serving to squelch debate and reify existing concentrations of power. How, then, can we make sense of the promiscuous possibilities of risk as a political resource?

The work of Ulrich Beck provides a useful set of concepts to navigate the promise and pitfalls of the politics of risk. Beck sees that new risks have the possibility of enlivening democratic politics. His central thesis posits that society is entering a period of late modernity characterized by the centrality of new forms of risk. For Beck, new forms of risk now sit at the center of political debate. While traditional political conflicts within modernity centered, to a large degree, on the distribution of "goods," such as wealth and jobs, Beck now sees the distribution of "bads"—forms of harm and danger—as central. As he writes:

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

> With the advent of risk society, the distributional conflicts over "goods" (income, jobs, social security), which constituted the basic conflict of classical industrial society and led to attempted solutions in the relevant institutions, are covered over by the distributional conflicts over "bads." … They erupt over how the risks accompanying goods production … can be distributed, controlled, and legitimized.[104]

Beck argues that as part of this turn, society can now be conceived of as a *risk society*. The production of new forms of risk, defined in keeping with the term's colloquial meaning as forms of harm and danger, are internal to the process of modernization—they are what Anthony Giddens refers to (in an unintended echo of the PCCIP's similar language) as the "dark side of modernization."[105] The production of risks is not a failure of modernization but rather a side effect. As Beck notes, "In advanced modernity the social production of *wealth* is systematically accompanied by the social production of *risks*."[106] The management of these sorts of risks is now a central feature and challenge of contemporary life.[107]

It is a provocative idea. For Beck, these risks are politically explosive. They have the potential to create institutional turmoil and disruption. Although forms of harm have, of course, always existed, a new category of risks—climate change, terrorism, systemic infrastructure failure, among others—are different. They are expansive—unmoored in time and space—global in scope, potentially catastrophic, and resistant to calculation.[108] These types of risk cannot be reduced to a specific location or fixed temporal period: to whom and where these harms might strike is not clear. Precisely *whose* problem such risks are is an open question.[109] Nor can they be reduced to easy estimates of frequency or degree of danger: they outrun our ability to tabulate either their likely occurrence or severity with great confidence.[110] These risks are atypical, infrequently occurring, and quite new, making historical extrapolation difficult.[111] As a result, uncontested statements about the danger they present are hard to offer. Calculability is central to the management of risks by supporting empirical testing and the provision of mitigation measures, including insurance. Absent accepted measures of probability, central institutions involved in managing risks—namely, branches of science, political bodies, and insurance—are destabilized.[112] In this manner, risks such as those associated with ecological collapse, nuclear waste, and terrorism, to select three risks Beck regularly invokes, undermine and challenge the ability of existing institutions. They create a crisis of legitimacy and a crisis of control.[113] Now, everything seems contestable and open to renegotiation.

New forms of risk hold out the possibility of radical change.[114] For a moment, as Beck writes, "The unthinkable and unmakeable become

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

possibilities."[115] The democratizing potential of risk operates across two distinct, though related, trajectories. On the one hand, risks can open previously closed domains and illuminate the political choices and implications buried beneath the surface.[116] The recognition of risks can draw attention to the political implications of seemingly private and apolitical areas and, in the process, can create openings for new political engagements at odds with the status quo.[117] Areas typically considered private and apolitical, such as business, economics, and science, are now politicized and subject to public scrutiny and discussion; they become legitimate topics of political discussion and intervention. As Beck notes, the recognition of new forms of risk can lead

> previously depoliticised fields of decision-making [to become] politicized.… Generally involuntarily and against the resistance of … powerful institutions … they are opening up these problems to public doubt and debates. In global risk society, therefore, subjects and themes once treated behind closed doors, such as public investment decisions, the chemical composition of products and medicines, scientific research programs and the development of new technologies, are articulated and debated in public.[118]

The recognition of the production of risks within areas considered private and "off-limits" illuminates the inherent politics at play. In doing so, it offers the possibility of opening these areas for participatory politics and some form of collective control. At the same time, risks also function as a resource for otherwise marginalized groups to enter into political discussions and coalitions. The recognition of novel risks enables new actors to enter the fray. The uncertainty surrounding the probability and effects of novel risks creates a space where new types of claims can be offered and taken seriously, and new sets of speakers can find a voice. New risks expand the horizon of possibilities and enable "as if" thinking. Once risks are publicly accepted and salient, a range of imagined possible scenarios are credible; as Beck notes, the subjunctive replaces the indicative mood.[119] In other words, novel risks enable a new type of thinking structured around the hypothetical or possible. If the past no longer is taken to offer a clear image of the future—if the future is no longer presumed to mimic the past—the limits of what is considered plausible are stretched. Claims and scenarios of what *could* happen are taken as legitimate. In this moment, new and existing social movements can adopt risks as a clarion call that challenges the accepted wisdom of the status quo and, importantly, challenges power.[120] The production of new risks creates seams where challenges to the authority and legitimacy of those in power are possible.[121] As Beck argues, "The boundaries between scientific

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and unscientific, between science and politics, and between experts and layman" erode.[122] Here, monopolies of knowledge are challenged and expert claims become contestable. This creates a space for new possibilities. Now a range of voices, including actors not typically authorized to speak with authority, are able to enter substantive debates.[123] In this respect, risks serve as a type of capital that is not reducible to existing political, economic, or scientific power.[124]

This optimistic portrait of risks must, however, be qualified. The political possibilities of risk are fragile and contingent. Risks are not inherently transformative; they offer the potential for political transformation. They are a resource open to appropriation, a source of legitimation and external support that actors of different stripes can highlight and rely on in advancing their positions. Risks are unreliable allies to power because their definition and interpretation do not necessarily follow established currents of power.[125] The potential of risks, for Beck, is the gap between what he terms *relations of definition* and other forms of power.[126] It is in this disjunction, between who defines risks and existing forms of power, that the radical potential of risks rests.[127] But what direction transformations linked to the recognition of novel risks will take—in support of democratization or the retrenchment of power; in favor of wise reconsideration or the headless rush of paranoia—is always an open question. The political potential of risks is simply that: *potential*. It requires organized interests to adopt risks and advocate for change.

Political, economic, and technological changes are creating new forms of peril that have real consequences and stakes. Yet, critically, these risks are always open to interpretation and mediation. That is, what risks mean and how they are thematized and translated into new policies and procedures is an open question. Risks do not in and of themselves compel action in particular directions; they can be used as symbolic resources for quite different ends.[128] The invocation of novel risks can support a reflexive democratic politics that considers the sources of new forms of danger and new courses of action or, alternatively, a type of totalitarianism that impoverishes participation in the name of emergency measures.[129] Democratization and contestability are useful and important correctives to the fencing off of political questions. But there are real and significant challenges that cannot be overlooked. If everything becomes open to questioning, then paranoia, conspiracy theories, and antiscientific crusades are also given room to flourish. In exploring the politics of risk, a set of key questions now slide into view: How, by whom, and to what end are risks interpreted and marshaled as a resource?[130] How have the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

exceptional circumstances of novel risk been fashioned into a durable set of security practices? And, most crucially, what social relations are embedded within new security practices? These questions provide useful guardrails for examining and understanding the implications of the new forms of infrastructure security that will transform the postal system, freight rail network, and electric power grid in the coming years.

Beck leaves us with a useful starting point: the ultimate significance of risks requires investigation into how groups mobilize around and deploy the symbolic currency or capital embodied within new risks. Once risks become relevant and salient—accepted as legitimate points of reference within the stock of common images, meanings, and arguments that define a shared culture—they can be adopted and wrenched to support new claims.[131] As certain risks are accepted as legitimate within the larger common culture, they can be appropriated by diverse sets of actors to justify action. In pointing out this dynamic, Beck is making a clear connection between two different understandings of culture—between viewing culture as a shared set of common, but by no means static or uncontradictory, meanings and culture as a repertoire of available tools. In this reading culture is shared, interpersonal, and collective: it is a broader structure within which action makes sense and is intelligible. In this fashion, Beck forwards a notion of culture that is compatible with Clifford Geertz's interpretive notion of culture as a shared semiotic framework or context within which action can be described.[132] Yet in identifying how cultural notions of risk can be instrumentalized as resources of legitimation, Beck shares an affinity with Ann Swidler (and others) in emphasizing how the broader set of available meanings within a culture enables and supports autonomy. In her well-worn phrase, culture acts as a "tool kit," a repertoire of available ideas from which individuals can draw to support actions. As Beck argues, risks empower marginalized groups because they offer "new sources of legitimation"—a new tool in the tool kit.[133] Risks "provid[e] political movements with the external conditions, strategies and resources for a type of 'judo' politics. That is to say … [risks] unleash powerful impulses for change from positions of relative powerlessness."[134] Here, culture does not compel action and is not deterministic or oppressive in a functionalist mode. On the contrary, it enables autonomy. It is through the availability of cultural resources that "strategies of action" can be forged.[135]

This view of the politics of risk is striking. It is at odds with how risk is usually thought to function within political life, particularly in the realm of national security policy and certainly in the context of post-9/11

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

security interventions. It is often taken as a given that new risks, emergencies, and security interventions lead to the suspension of democratic processes. In moments of peril, it is said that the powerful are uniquely positioned to seize power. This view abounds. The concept of *securitization*, developed most centrally within security studies by Barry Buzan, Ole Waever, and Jaap de Wilde, suggests that security is, primarily, a rhetorical device used to justify exceptionality in support of the powerful.[136] Studies of securitization see "security" as a trump card used by the state to suspend the regular features of governing and seize power. As Buzan and colleagues note: "'Security' is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics."[137] In this thinking, security necessarily blunts normal democratic mechanisms. As Buzan and coauthors remark:

> Securitization … means to present an issue as urgent and existential, as so important that it should not be exposed to the normal haggling of politics but should be dealt with decisively by top leadership prior to other issues. … It works to silence opposition and has given power holders many opportunities to exploit threats for domestic purposes, to claim the right to handle something with less democratic control and constraint.[138]

This notion of the politics of risk—as something inherently antidemocratic—has been widely adopted by observers of the post-9/11 moment. In *Fear: History of a Political Idea*, Corey Robin critiques at length the notion that fear and risks—particularly the risk of terrorism post-9/11—can serve as the foundation for democratic revitalization and engagement.[139] For Robin, risks are the exclusive province of the powerful; anxiety, fear, and uncertainty only support greater concentrations of power and are put in service to reduce public participation and freedom.[140] In Robin's reading, risks obscure the political character of situations and justify the suspension of normal democratic processes in response to the needs of a presumed emergency. John Mueller in *Overblown* offers much the same argument in reference to post-9/11 politics, and certainly, many examples of how risks have been used to justify exceptionality at the expense of democracy can be offered.[141] But these accounts adopt either implicitly or explicitly a somewhat limited notion of culture. In these, iterations culture is little more than the scrim through which the powerful impose their prerogatives. This view is blinkered. Culture is more than the distillation of the ideas and notions the powerful hope to promote. Culture is rich and messy: it contains contradictory ideas and arguments. It is, following James Carey's discussion of a cultural approach to communication, a shared set of meanings that provide the larger context within which ideas

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and arguments make sense.[142] Once risks are publicly salient—once they have moved from being on the edge of legitimate discourse and are more or less taken to be true and have taken up residence as part of the larger shared culture—they are no longer the province of a particular speaker. In these moments, the stakes are high. Both the powerful and the marginalized can fight to appropriate the language of risk for their own ends. The powerful can claim that exceptional circumstances require setting aside democratic norms and processes. They can (and often do) cloak their agenda in the language of risk and use it as a means to accumulate or consolidate power. But those outside of power can also enact securitization—they can speak the language of security and exceptionality as a way of challenging the existing status quo. Securitization can work not only to silence but to amplify voices. The exploitation of threats can be put into the service of democratic participation. Risk, in and of itself, does not compel a particular outcome. What is left then is a demand for close examination how risks circulate and are deployed. This is precisely the task to which the following chapters turn. After 9/11 the cultural reframing of infrastructures as dangerous things and the creation of institutions that supported this view were firmly put in place. These changes set the stage for a significant transformation: a possible reordering of the material outlines and power dynamics that defined infrastructure. How this transformation would unfold, however, was an open question.

Infrastructure Inversion and the Politics of Post-9/11 Security

After the attacks of September 11, infrastructures were recast as sites of vulnerability, danger, and fear. This reordering was driven by clear choices—specifically the decision of the Bush administration to adopt the PCCIP's (and other earlier groups') framing of infrastructures as sites of danger and the subsequent decision to make infrastructure protection a clear, and well-funded, government priority within DHS and across the federal government. The difficulty in calculating the risk of terrorism became an acute problem; the possibility, rather than the probability, of catastrophic loss became a source of concern for the state, operators, and a host of publics associated with these networks. This was a rich moment. The political possibilities of risk described by Beck came alive. As infrastructures were revisited or redefined as sites of anxiety and danger—targets in waiting—they suddenly became open to reconsideration and remaking. The sunk politics of infrastructure, at least for a moment, would become visible; the upheavals of deregulation would reemerge as public

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

problems. The cultural and institutional reframing of infrastructures as dangerous objects created a crisis of control: it opened infrastructures up to competing claims about how they should be organized; it created an opportunity for otherwise marginalized voices to be heard; and it created an opportunity for new, surprising political coalitions to crystallize. It created real possibilities for change—possibilities that were not anticipated during the initial rush to include infrastructure protection within an expanding portfolio of homeland security during the early years of the Bush administration. During these early post-9/11 days, much remained unclear. How and on what terms would infrastructure security unfold? Who would define the contours of these new security measures? How would new, enhanced forms of security square with the needs of access, low cost, and reliability (among other values)? Importantly, what type of social relations would these new security interventions codify? Infrastructures are a nest of technical and nontechnical elements; they join together technical artifacts, legal standards and regulations, infrastructure owners, different sets of users and customers, and labor in a contingent set of relationships. How would new security interventions reorganize these relationships? In short, how would infrastructures order?

The answers to these questions would only gradually become clear in time. During the Bush and then Obama administrations (and as of this writing, the Trump administration), critical infrastructure protection would remain a key priority and point of fierce debate. The following three chapters explore in detail how new security concerns upended and eventually remade the postal system, the freight rail network, and the electric power system. They trace the *bureaucratization of risk*: how the abstract threat of terrorism—the idea of a possible terrorist attack at some point in the future—is written into stable and routine security practices, regulations, codes, and technologies. This process was contradictory. It led to both the opening of sealed domains and a type of democratic revitalization that challenged the changes unleashed through deregulation, and it also led to the further consolidation of power to control infrastructure. Indeed, in time both the promise and fragility of the politics of risk would become clear.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

4

Infected Mail: Labor, Commerce, and the 2001 Anthrax Attacks

Every postal worker that has anything to do with the mail is on the front lines.
—David Galvin, United States Postal Service worker, Waltham, Massachusetts, 2001[1]

In 2001 an unknown number of letters containing spores of anthrax were sent through the U.S. postal system, exposing scores of postal workers and patrons to possible harm.[2] Five individuals died as a result of anthrax exposure (22 were infected) while over 30,000 people were given prophylactic antibiotic treatment.[3] According to estimates compiled by the National Research Council, one-third of the U.S. population took extra precautions in handling the mail during the attacks.[4] The economic impact of the attacks was staggering: postal facility cleanup ran into the hundreds of millions of dollars while declines in letter volume, productivity, and new security measures amounted to roughly $6 billion.[5] Suddenly, one of the more mundane aspects of daily life—opening the mail—became imbued with danger and unease. Panic ran high: hoaxes and false alarms involving letters thought to contain anthrax became common disruptions; the investigative arm of the United States Postal Service (USPS), the United States Postal Inspection Service (USPIS), dealt with over 17,000 such incidents and evacuated over 600 postal facilities in the year following the attacks.[6] As Chief Postal Inspector Lee Heath noted, the anthrax letters were a "weapon of mass disruption."[7] While not reaching catastrophic levels of harm, the tragic deaths of five individuals, compounded by widespread anxiety and far-reaching economic consequences, elevated the attacks into a disaster. The attacks destabilized the continued flow of mail; imperiled, to a degree, the health of workers and patrons; and introduced potentially ruinous costs for the already financially precarious USPS.

In response to the attacks, USPS adopted new technologies to counter further incidents of biological terrorism. The attacks—occurring just

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

days after the terrorist strikes of 9/11—were initially viewed through the prism of international terrorism. Policy-makers interpreted the letters as indicators of the rising terrorist threat.[8] Defense officials and public health experts had prepared for a possible biological attack involving anthrax for decades. The 2001 attacks, however, highlighted the limitations of these preexisting biodefense efforts and revealed the drawbacks of deregulation (see chapter 2). The postal system's reliance on automation and centralized processing centers actively facilitated the spread of anthrax throughout the country. USPS eventually installed two new surveillance systems—the Biohazard Detection System (BDS) and Intelligent Mail—to counter future attacks. These systems of control transformed the operation of the postal network in explicit and subtle ways. They embody clear political choices and commitments: new forms of postal security now privilege particular types of uses and users at the expense of others, sort suspect or at-risk network flows from "normal" and accepted flows, and prioritize particular types of threats while ignoring others. It is within these new standards that the legacy and politics of disaster are recorded and made durable.

* * * *

The following chapter begins our consideration of how post-9/11 security interventions reflect upon and are in dialogue with the upheavals of deregulation. Deregulation transformed the material operation of infrastructures and the organization of power within these networks. It created networks susceptible to large-scale failure and, equally important, it created new hierarchies of power within these systems. In each case—the postal service, freight rail network, and electric power system—the new forms of security built into the day-to-day operations of these networks wrestle with the consequences of deregulation. The post-9/11 debates about infrastructure security are, in a meaningful way, a referendum on the wisdom, consequences, and viability of deregulation.

This chapter examines the politics of new forms of postal security. It looks at the failure of pre-attack planning to anticipate the unique challenges of the 2001 anthrax attacks and traces the contested creation and installation of the BDS and Intelligent Mail. It considers how, by whom, and to what end new control technologies have been integrated into the postal network. Evaluating these systems highlights how disasters and new perceptions of risk can become encoded within new infrastructure standards. As Susan Leigh Star points out, behind the seemingly mundane and normal working of infrastructures rest explicitly political decisions

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

that are all too often overlooked.[9] Opening the "black box" of infrastructure standards uncovers conflicts and constitutive choices that otherwise remain below the surface. Peering within the inner workings of new postal security practices reveals the reentrenchment of powerful interests. The adopted forms of surveillance reproduce the prevailing hierarchies of power that have dominated postal politics since deregulation. The centrality of large commercial mailers, the ongoing subordination of other publics, specifically labor, and the marginalization of other concerns or values in favor of market considerations find clear expression within the BDS and Intelligent Mail. While in rail and electric power, new concerns over security would eventually serve to create new spaces and mechanisms devoted to public accountability, here, after a brief moment of promise, the door slammed shut.

The process through which new forms of security emerge is never simple or inevitable. How to build new security standards into the postal network—determining what constitutes an acceptable "fix" for the problem of biological terrorism—was an open question subject to intense debate among postal management, commercial interests that used the network for business, and postal workers. As chapter 3 made clear, novel risks alone compel very little. Risks circulate in unpredictable ways: alternately providing an impetus for new political engagement and the reordering of power or, conversely, serving as a means for foreclosing political deliberation and reifying existing centers of power. It is how risks are seized and translated into action that shapes their lasting significance. Tracing the adoption of the BDS and Intelligent Mail underscores the relevance of this insight. As we will see, key infrastructure publics are central in dictating how the disruptive potential of risks is concretized into routine practices.

Old Fears and New Challenges: The 2001 Anthrax Attacks and the Limits of Planning

The anthrax attacks of 2001 were, in many ways, unsurprising. Defense strategists and public health officials had worried about the possibility of a biological attack since at least World War II. Anthrax, due to its durability and relative ease of production, often topped the list of likely agents to be used. As two analysts for the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) summarized: "Anthrax, in the minds of most military and counterterrorism planners, represents the single greatest biological warfare threat."[10] Historically, planners assumed that

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

an attack using anthrax would fall into one of two categories: a mass-casualty attack targeting a large concentrated population or a limited-exposure attack, perhaps using letters containing anthrax, targeting a small number of individuals. While the mass-casualty scenario received far greater attention—and had a much longer history—both models led to the development of preparedness efforts.[11]

Thomas V. Inglesby, writing in *Emerging Infectious Diseases* in 1999, offers a narrative description of the mass-casualty scenario:

> On the evening of November 1, a professional football stadium before an audience of 74,000. The evening sky is overcast; the temperature mild, a breeze blows from west to east. During the first quarter of the game, an unmarked truck drives along an elevated highway a mile upwind of the stadium. As it passes the stadium, the truck releases an aerosol of powdered anthrax over 30 seconds, creating an invisible, odorless anthrax cloud more than a third of a mile in breadth. The wind blows the cloud across the stadium. … The anthrax is detected by no one.[12]

Similar speculative scenarios circulated within U.S. defense, public health, and scientific communities during the Cold War, appearing in public information campaigns produced by the Federal Civil Defense Administration and the Department of Defense and serving as the basis for numerous tests undertaken by the U.S. and the World Health Organization (WHO).[13] After the Cold War, the model was again cited to caution against the insecure stocks of bioweapons in the former Soviet republics, the threat posed by so-called rogue nations (such as Iraq), and terrorist organizations.[14] In each instance, planners presumed that an attack would target an area with a high population density, such as a subway or stadium, in order to inflict maximum harm.

A series of hoaxes during the late 1990s pointed toward another model of attack—limited exposure—and highlighted the possibility that the postal system could be used to spread anthrax. During this period, letters purporting to contain anthrax were sent to government offices, health clinics, and private businesses throughout the U.S. and Canada.[15] Although none of these letters actually contained anthrax spores—they were doctored in most instances with a harmless powder—the hoaxes pointed toward a model of attack that was far different from the continually recycled "mass-casualty" scenario. Public health officials and postal management took note. They began to consider the possibility of a narrowly targeted attack delivered through the mail.

The mass-casualty and limited-exposure models underpinned different public health interventions.[16] The mass-casualty model sat behind

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

a number of high-profile efforts, including the creation of the Centers for Disease Control and Prevention (CDC) Epidemic Intelligence Service (EIS), which placed epidemiologists in the field to watch for signs of a biological attack; the establishment of the National Pharmaceutical Stockpile; and the organization of special biohazard rapid-response teams.[17] In 1999, in response to the anthrax hoaxes, the CDC released interim guidelines outlining how to respond to alleged incidents of anthrax in the mail.[18] USPS subsequently adopted the CDC's recommendations and issued a new management instruction, "Emergency Response to Mail Allegedly Containing Anthrax," in October of the same year.[19] The new policy was simple: in the event of the discovery of a suspect piece of mail, workers were to notify their supervisors, isolate the area containing the suspicious item, and wash their hands. [20]

The Limits of Normative Cases: The 2001 Anthrax Attacks

In the fall of 2001, the possibility of an anthrax attack ceased to be purely hypothetical. In late September and early October, letters packed with anthrax were sent to various media outlets in New York and Florida and to the offices of Senators Tom Daschle and Patrick Leahy.[21] The actual attack looked much different from the established scenarios. It was neither a large-scale release nor a single instance of limited exposure. Both the mass-casualty scenario and the limited-exposure model assumed a single moment of peril and a limited, well-defined radius of exposure. The 2001 attacks were different. The anthrax letters seemed to "infect" the entire postal network through cross contamination. As the malicious letters were processed, anthrax spread to other letters and postal equipment. Rather than subjecting a narrowly defined population to exposure or affecting a few well-defined "at-risk" sites, cross contamination potentially exposed everyone who came into contact with the postal system to harm.[22]

The attacks exploited the particular architecture of the contemporary postal system (see chapters 1 and 2). Beginning in the 1970s, USPS invested billions of dollars in the adoption of automated equipment in order to streamline postal processing.[23] By the late 1990s, the postal network was structured around massive centralized processing plants that relied on automated equipment. The mechanics of automated processing in these dense hubs made the network cheaper and more efficient, but it also facilitated cross contamination as spores of anthrax escaped and mixed with the regular mail. High-speed automated processing rapidly compresses letters, forcing air and, in the case of sealed envelopes filled with anthrax, spores of anthrax out through minute tears and pores in the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

envelopes. These spores then traveled through the air, contaminating other pieces of mail, processing equipment, and the larger postal workspace. Spores eventually spread to over 60 different locations in six states.[24] Anthrax appeared in disparate places—the Federal Reserve Board, Howard University, Walter Reed Hospital, a home in rural Connecticut, to name a few—linked only by the common thread of postal service.[25] CDC director Dr. Jeffrey Koplan offered a bleak assessment, stating that "there seems to be the potential for not just hundreds and just thousands, but tens of thousands and maybe more letters to be potentially at risk for some level of cross-contamination."[26] Cross contamination revealed a hidden downside of deregulation: the adoption of automation and centralized processing and the pursuit of more efficient network operation had created new vulnerabilities for the anthrax letters to exploit and amplify.[27] The attacks, in this fashion, illustrate Ulrich Beck's wry observation that it is the very triumphs of modernization that now produce new forms of risk.[28]

The protocols developed by the CDC and USPS in response to the hoaxes of the late 1990s offered little comfort. They had assumed that only a letter deliberately treated with anthrax was dangerous. Importantly, in-place emergency response procedures also assumed that anthrax exposure would be obvious: previous hoax letters had contained explicit threats and noticeable heaps of white powder. It was assumed that a person who came into contact with an anthrax letter would be well aware of their exposure. Neither the CDC nor USPS had previously considered the possibility of cross contamination.[29] As instances of cross contamination began to appear, U.S. Surgeon General Dr. David Satcher noted the rapidly shifting landscape: "Until a week ago, I think all of the experts would have said [that cross contamination was not a danger]. The fact of the matter is, we were wrong."[30] Cross-contaminated mail did not bear suspicious markings, threatening language, or other outward signs of malicious intent. Spores of anthrax in low, though still dangerous, quantities were invisible to the naked eye; cross-contaminated mail appeared indistinguishable from the familiar mix of bills, letters, and magazines that typically arrived in mailboxes across the country. A person receiving a cross-contaminated letter would likely be unaware of the exposure. Cross contamination placed postal employees at risk as well. Workers laboring in proximity to contaminated automated equipment faced unwitting exposure. With each new case of cross contamination, the limitations of the CDC-USPS guidelines became increasingly apparent.[31] New forms of security would have to be created.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Searching for Security: Risk and Infrastructure Publics

The anthrax attacks, in isolation, compelled little action. The content of new security protocols was an open—and contentious—question. While the 2001 attacks revealed the limitations of in-place protocols, what was to come next—the shape of a new security posture—was by no means clear. The two infrastructure publics most closely linked to the fortunes of the postal network—postal workers and the commercial mailing industry—wrestled to define the terms on which new forms of postal security would rest. Labor and commercial mailers viewed the problem of biological terrorism through starkly different lenses: workers viewed it as a workplace safety issue, while the mailing industry—companies relying on mailings as a central component of their business, including direct mailers that advertise for clients and catalog merchants—worried about disruptions to the smooth functioning of the postal network. These interpretations focused on different objects of concern—the protection of worker health, on the one hand, and the preservation of network functionality, on the other—and, unsurprisingly, led to disagreements over the contours of new security standards.

Unions representing postal labor viewed the attacks as assaults on the postal workforce. Labor was sharply critical of the initial failure of postal management to contain the spread of anthrax (see figure 4.1). Cross contamination affected postal workers directly: nine postal workers contracted anthrax from cross contamination, and testing eventually confirmed the presence of anthrax in over 23 different postal facilities.[32] The American Postal Workers Union (APWU), the largest postal union, led a walkout of workers in New York City and filed three lawsuits in U.S. district courts, charging USPS with failing to provide a safe workplace.[33] APWU president William Burrus publicly accused postal management of offering different levels of safety for government officials and postal workers. Burrus pointed out that the Supreme Court and congressional offices were closed at the first hint of possible anthrax exposure, while postal facilities, in some cases, remained open even after anthrax had been discovered. As Burrus framed the issue: "Are the lives of postal workers less valuable than the lives of U.S. senators? Are the lives of postal workers less valuable than the lives of Supreme Court justices? What value do our lives have?"[34] William Smith, president of the New York Area Metro Postal Union, drew the same conclusion, tartly offering: "I realize that [postal] employees are not Supreme Court justices or senators or Congress, but they are God's children; they have the same right to life as the aristocrats" and that "no one piece of mail is worth a human life."[35]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Figure 4.1
Postal employees picket outside the post office building in Eatontown, New Jersey, November 1, 2001. Image courtesy of June Mckim/Getty Images.

While labor viewed biological terrorism as an attack on the bodies of postal workers, the mailing industry saw the "health" of the network as the central object in need of protection. This concern—over network functioning—fit well within the crystalizing logic of the moment. President Bush had quickly worked to emphasize notions of what Andrew Lakoff describes as the logic of "vital systems security" in the aftermath of 9/11 (see chapter 3).[36] The recasting of infrastructures as dangerous spaces that needed protection from external threat (namely terrorism) stood in opposition to logics more plainly structured around the protection of populations.[37] Commercial mailers moved to protect the network. They worried that if the public lost confidence in the safety of the mail—refusing to accept "junk mail," catalogs, and other forms of mail out of an abundance of caution—their businesses would be destroyed.[38] Trade associations such as the Association for Postal Commerce, Mailers Council, and the Direct Marketing Association called for postal management to take steps to quell safety concerns. Yet commercial mailers also worried about the side effects of new layers of security. They warned that adopting poorly

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

designed security efforts could jeopardize the two qualities that made the mail an attractive commercial medium: low cost and timely delivery.[39] The concerns of large bulk mailers were not to be taken lightly: by 2001, roughly 75% of all mail was sent by bulk mailers.[40] Large commercial mailers have historically played a significant role in dictating postal policy. The regulatory reforms of the 1970s and 1980s enhanced their power while marginalizing other publics and visions of postal service (see chapter 2). Although both labor and industry advocated for new forms of postal security, commercial mailers offered a crucial caveat: new security measures could not increase the postage rates charged to large bulk mailers or impose delivery delays.[41] Commercial mailers wanted new forms of security to restore confidence in the mail while preserving the speed and economy of the network.

The Postal Service found itself in a difficult position. Its two most powerful and vocal constituents, labor and large mailers, aggressively pushed for new forms of security—implicitly and explicitly questioning postal management's initial response to the attacks—although their aims chafed. Labor's prioritization of worker safety would likely lead to added costs and delays in postal processing; mailers called for security but refused to accept new practices that would add costs or jeopardize the speed and convenience of the mail. In order to reconcile this tension, the head of USPS, Postmaster General Potter, created a new working group, the Mail Security Task Force (MSTF), in October 2001 to consult with the Postal Service on new security practices.[42] The task force broke with long-standing postal policy and brought together management, senior leadership from the postal labor unions and management associations, and representatives of the mailing industry.[43] This was a significant change. For decades, powerful mailers had enjoyed exclusive access to postal management through the Mailers' Technical Advisory Committee, a public-private partnership run by the mailing industry and the Postal Service that was closed to union participation.[44] The MSTF was different: it included both union leaders and the voices of commercial mailers.

The MSTF underscores the political potential and limitations of novel forms of risk. In this case, labor's agitation sparked institutional innovation. The anthrax attacks, and the uneven initial response by USPS, provided labor with a highly visible management "failure." Postal management's initial inability to grapple with cross contamination allowed labor to level powerful charges of unequal treatment. The larger backdrop of the unfolding war on terror and a ramping up of concern over homeland security was baldly significant. The recasting of infrastructures

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

of dangerous things seemed to find its perfect expression in the 2001 anthrax attacks: *even the postal system* could be a target. Against this backdrop, postal workers struck a different note than commercial mailers. Workers made it clear—they *were* the network. Commercial mailers posited a view of the postal network that was depopulated—their concerns over the smooth functioning of the network glossed over the people that actually made the system work. Workers were explicit: it was their bodies that were imperiled by the anthrax attacks. Labor seized on the salient threat of terrorism to upend the status quo and, briefly, secure a more prominent place in postal policy. Risks can, in certain instances, serve as a catalyst that supports the democratization of formerly closed institutions (see chapter 3).[45] Postal workers leveraged safety concerns to wedge open postal governance. While in other domains invocations of security post-9/11 were used to justify the foreclosure of political participation due to "exceptional" circumstances, here, something different seemed, at first, to unfold. The MSTF, on its face, offered a more democratically minded form of governance that at least nominally enfolded those most directly subject to the bodily harm inflicted by the anthrax attacks—postal workers—within its deliberations. In this manner, security concerns appeared for a moment to lead to new types of accountability.

Yet the power of the MSTF was circumscribed. The MSTF's recommendations were informal and nonbinding; the Postal Service retained final authority over security policy. The invitation to join the MSTF placated the concerns of postal workers for a time. Now, finally, labor could join commercial mailers in providing postal management with advice outside of highly formal rate cases or the negotiation of collective bargaining agreements. However, postal workers soon realized that access is not quite the same as power. Labor would quickly find out that commercial mailers still held the power to shape postal policy. Risk, as a political resource, transformed to a limited degree the governance structure of postal decision-making, but as newly adopted security standards would make clear, in this case risk did not reorganize the basic structure of power within postal politics. A moment of possible transformation and reordering would slip through the fingers of postal workers.

From Irradiation to ICTs: The Politics of Selection

USPS, with the assistance of the MSTF, considered a number of possible "technical fixes" to the problem of biological terrorism, including a host of sanitation technologies, process changes, and information and communication technologies (ICTs) that provided surveillance and detection

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

capabilities.[46] The eventual adoption of ICTs over other competing technologies was neither inevitable nor obvious. Rather, the key ICT systems finally installed, the Biohazard Detection System (BDS) and Intelligent Mail, emerged largely thanks to the efforts of commercial mailers and the timely intervention of external groups, including congressional staffers and select local governments. The adoption of the BDS and Intelligent Mail was a clear triumph for commercial mailers. Unlike competing technologies, ICTs offered the promise of seamless operation—security that did not disrupt the flow of mail—and did not saddle commercial mailers with burdensome additional costs. As security technologies, they prioritized the "health" of the network over the prevention of physical harm to postal workers.

The reliance on ICTs was a reversal. Initially, postal management looked to sanitation technologies, irradiation in particular, as the most promising security option.[47] Irradiation uses targeted ionizing radiation to kill or neutralize harmful biological agents. It is routinely used in industrial settings, such as food processing and medical equipment sterilization.[48] Unquestionably, irradiating mail would destroy any spores of anthrax.

Widespread adoption of irradiation faced stiff opposition. USPS began irradiating mail sent to federal agencies in November 2001.[49] Operational problems and safety concerns marred efforts to expand the use of irradiation to cover the entire postal network. Delays were rampant. Mail subject to irradiation took over twice as long, on average, to reach its final destination (eight days, as opposed to two or three days).[50] For commercial mailers, the side effects of irradiation were even more troubling. Irradiation damages routine items sent through the mail. Plastics (such as credit cards), electronics, and other materials sent through the mail experienced varying degrees of damage.[51] Even regular letters could become brittle and discolored as a result of the process.[52] Irradiation sanitized the mail at the expense of damaging, and in some cases rendering useless, the contents of the mail. Shortly after the introduction of irradiation for federal mail, commercial mailers argued against expanding the program.[53]

Federal employees and local governments provided mailers with support. They were also hostile to irradiation. Federal employees receiving irradiated mail claimed that it caused nausea, headaches, nosebleeds, and other forms of sickness. Both the Congressional Office of Compliance and the National Institution for Occupational Safety and Health opened investigations into the possible side effects of handling irradiated mail.[54] Both reviews noted no known long-term health effects associated with irradiated mail but concluded that handling such mail may have caused the reported health symptoms.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Local governments were nervous about irradiation as well. They were not eager to have irradiation facilities operating in the midst of their communities. In order to test the feasibility of expanding irradiation system-wide, USPS invested $40 million in new equipment and began constructing specialized facilities near Washington, DC. Local officials reacted swiftly. One week after USPS started outfitting a new sanitation facility in Temple Hills, Maryland, local officials shut off the building's utilities in response to concerns over the safety of bringing "at risk" mail into the county. Local officials in Montgomery County, Maryland, similarly derailed USPS plans to operate an irradiation facility.[55]

The combination of operational problems, health concerns, and local opposition blunted efforts to implement system-wide irradiation.[56] USPS shifted course and embraced a strategy primarily focused on ICTs. The BDS and Intelligent Mail emerged as a palatable alternative to sanitation technologies. As a technical "fix" to the problem of biological terrorism, they promised security without upsetting day-to-day operations or, importantly, increasing the costs ascribed to large mailers. Both the BDS and Intelligent Mail are political artifacts that in different ways embody the triumph of bulk mailers at the expense of postal labor and, to a degree, the general public. Encoded within these new infrastructure standards were implicit and explicit political judgments about the relative importance of the commercial features of the postal network and the safety of workers, assessments of how to define "safe" and "at-risk" mail, and assumptions about who should ultimately be responsible for the costs of added layers of security. Labor leaders felt an acute betrayal. While the MSTF promised them a more active role in postal governance, the shift to ICTs, in their estimation, bent to the demands of powerful mailers at the expense of workplace security.[57]

Toward a Bifurcated Postal System: The Biohazard Detection System

The BDS is an automated detection system that tests air particles above automated mail-processing equipment for the presence of anthrax and, in the event of a positive result, triggers on-site and off-site alarms.[58] Effective lobbying by commercial mailers guided key decisions concerning the system. The BDS splits the postal network into two separate processing networks: one for individuals and small organizations sending mail from their homes, street collection boxes, or post offices and another for commercial mailers sending letters in large batches at discounted rates. The BDS, and its associated costs and extra handling, apply only to the first, as bulk mailers are able to opt out of the costs and extra handling tied to new security screening. The BDS treats mail originating from large

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

mailers as safe while scrutinizing the mail from individuals, homes, and other small entities. The interests of large commercial mailers are embodied in the BDS: it provides a measure of security designed to reassure the public that the mail is safe but does so without adding to the postage rates or delivery times of bulk mailings.

USPS and Northrop Grumman began developing the BDS in 2002; it became fully operational in 2005.[59] The BDS is installed in large postal Processing and Distribution Centers across the country. The BDS is attached to specific pieces of automated postal processing equipment, Advanced Facer Canceller System (AFCS) machines, which scan mail for proper postage. The mechanics of the BDS are straightforward (see figure 4.2): as letters are processed on an AFCS, air samples are continually collected by the BDS and analyzed for the presence of anthrax. A positive test signal stops mail-processing equipment, triggers alarms within the facility, and notifies emergency responders.[60] The system allows the AFCS to operate at regular rates and, absent a positive result, does not delay mail flow.[61]

Deciding where to place the BDS within the postal processing chain—and on which pieces of automated equipment to attach the BDS—is

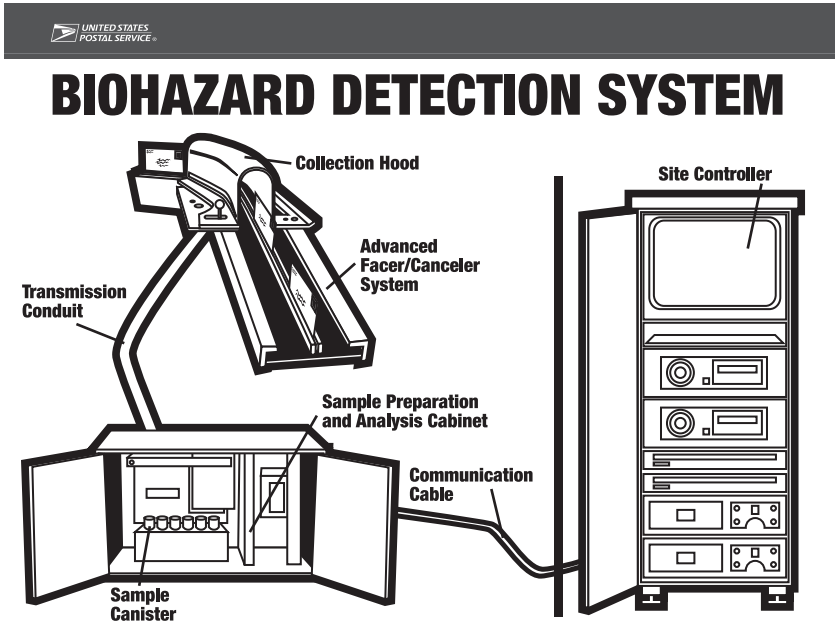


Figure 4.2
Biohazard detection system diagram. Image from the USPS.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

significant. Deciding where to locate the BDS rests on assumptions concerning which mail is considered "at risk" and, crucially, determines who is responsible for the costs associated with the provision of security. The decision to integrate the BDS with the AFCS, rather than other pieces of automated postal machinery, was not guided by the technical features of automated equipment, the precise outlines of the 2001 attacks, or even intelligence reports concerning how a future attack may unfold. Indeed, AFCS machines are only one of many different pieces of automated equipment that process mail. What is unique about AFCS machines, however, is that they exclusively process collection mail—letters sent from street collection boxes, homes, small businesses, and individuals—while other automated equipment, such as delivery bar code sorters (DBCS), process both collection mail and bulk mailings from large mailers. By placing the BDS on the AFCS, the BDS only "scans" collection mail and avoids bulk mailings.[62] AFCS machines, however, are not the only type of automated equipment that can cause cross contamination. During the 2001 attacks, both AFCS and DBCS machines cross-contaminated postal facilities.[63] Although in 2001 the majority of anthrax letters were sent through collection mail, at least one mailing was sent as a parcel (a category of mail that is not currently subject to the BDS).[64] USPS did collect intelligence to assess the threat of another bioterrorist attack using the mail, but the independent contractor did not complete the assessment until May 2003 and presented it to USPS in June 2003—nine months *after* the outlines of the BDS were approved by USPS management.[65]

The organization of the BDS reflects the wishes and power of large-volume mailers to define new security standards. The power they attended during the political restructuring of the 1970s and early 1980s has not abated. Here, large-volume mailers again flexed their power to shape postal policy and the adoption of new technologies. As first became clear through their opposition to irradiation, industry trade groups sought to avoid any costs or delays associated with added security. They argued that bulk commercial mailings were safe, while collection mail was potentially dangerous.[66] By bypassing the BDS, bulk mailers avoid the added costs associated with security. The costs of the BDS are not included in bulk mail rates. These costs are not trivial: according to audits by the USPS Office of Inspector General (OIG) and published figures from the *Washington Post*, total system costs range between $1.05 and $1.4 billion, with continuing operating costs above $100 million annually.[67] While a fraction of these costs have been paid through federal appropriations, the majority of the costs, including annual operating costs, are expenses

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

recovered through standard postal rates.[68] With bulk mailers effectively opting out of the BDS, the system's costs are borne by individual mailers and small entities that do not have the opportunity of opting out and, to a lesser degree, the public through limited federal homeland security appropriations. In place of involvement with the BDS, large mailers have the option of enrolling in a voluntary mail security program—known as the B.2.2 Security Initiative for Commercial Mailers—that offers participants confidential and nonbinding security recommendations.[69]

While industry trade groups initially joined labor in supporting new security efforts as a means of assuaging customers' fears of anthrax, they successfully worked to limit the scope of new security practices and displace the costs onto the public at large (through appropriations) and small and individual mailers. While the threat of biological terrorism briefly served to democratize postal governance and make the service newly accountable to a broader cross section of key publics, the BDS demonstrates the limits of risk as a disruptive or transformative political resource. At its core, the BDS is a conservative response to the attacks: it reinforces the privileged position that commercial mailers hold in postal politics. In its selective deployment and distribution of costs, the BDS creates a tiered system of security within which bulk mailers are free from added burdens. The USPS OIG and postal labor unions criticized the exclusive application of the BDS to collection mail and called for an assessment of all categories of mail.[70] APWU president Burrus noted the following during congressional testimony:

> [The BDS] will go on specified postal equipment, not all of the equipment. … Over 50 percent of [mail] bypasses the [BDS]. … That mail would never come through … biodetection equipment. It will go directly to the letter carrier, to the bag, to the American customer, to the American citizens.[71]

Burrus's estimate may have been generous: mail sent from (largely commercial) mailers at bulk rates—roughly 75% of all mail—avoids scanning by the BDS.[72] In calling for an expanded program of detection, the USPS OIG and the APWU highlight the political choices inscribed within the BDS.

Intelligent Mail: Revenue, Cost, and Security

The BDS was not the only new security system adopted after the anthrax attacks. Postal management also introduced a new suite of services, known as Intelligent Mail, to confront biological terrorism. Intelligent Mail is an assemblage of interlinked technologies—including data-rich bar codes, scanning equipment, and software—that generate, store, and manipulate real-time data from the postal network. As a security tool,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Intelligent Mail data can be used to reroute mail flows away from "trouble areas" where anthrax has been identified. This allows investigators to reconstruct the path of contaminated mail through the system. Intelligent Mail is, however, not exclusively a security technology: it also serves as a tool for revenue generation and cost control. It fuses what are typically discrete domains of surveillance: consumptive behavior, the workplace, and security.[73] Intelligent Mail underpins the production of new product lines and new forms of workplace control. It is part of a larger, ongoing transformation of postal service into a "flexible" enterprise that is less hospitable toward a unionized workforce and less interested in providing uniform services to a broad customer base. While the politics of the BDS are largely defined by absence—the ability of large mailers to opt out—the politics of Intelligent Mail are defined by those it includes, both as customers of newly designed commercial products and as subjects under supervision. Intelligent Mail produces a specific matrix of social relations: within its operation, we find the concurrent prioritization of commercial interests and the marginalization of labor. Here, as in the BDS, we find the politics of disaster encoded within the workings of new infrastructure standards.

The development of Intelligent Mail began in the mid-1990s as a joint effort of postal management, commercial mailers, and postal equipment manufacturers. Initially, the project had little to do with security. The aim was to create new value-added products for commercial mailers and new managerial tools for USPS to control costs.[74] The 2001 anthrax attacks pointed out another application for the developing technology: security. Postal management and the mailing industry scrambled to reposition Intelligent Mail as a security technology, arguing that its security applications were a "logical extension" of its commercial and operational aims, and pushed for its adoption in the March 2002 *Emergency Preparedness Plan*.[75]

After a decade of development, Intelligent Mail launched in 2006 (see figure 4.3).[76] Intelligent Mail aims to create a perfect real-time rendering of the postal network that USPS refers to as *total mail visibility*. Intelligent Mail combines new information-rich bar codes, scanning equipment, and computer systems to create and manage data charting mail flow and worker behavior.[77] Intelligent Mail bar codes contain a range of information—including a unique identifier indicating mailer and recipient, routing details, and service type—and are placed on individual pieces of mail and aggregates, such as transportation containers. As mail moves through the network, automated processing equipment and postal workers using handheld scanners, known as Intelligent Mail Devices, scan bar codes to create detailed real-time records of postal operations.[78] Intelligent

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Intelligent Mail® Vision
what's going on with your mail?
INTELLIGENT MAIL® VISION
imagine the possibilities
Intelligent Mail® Vision
bringing Xtreme visibility into the mail
UNITED STATES POSTAL SERVICE®
What is the Intelligent Mail® Vision?
The Intelligent Mail Vision provides end-to-end visibility of the mail. From a seamless process for mail acceptance to delivery using standardized Intelligent Mail barcodes, continuous tracking, and mail quality feedback and service measurements, the Intelligent Mail Vision positions letters, flats and parcels as a key communications medium.
How do we achieve visibility?
Applying a unique Intelligent Mail barcode on each mailpiece and mail aggregate allows the U.S. Postal Service® to scan, track and capture data on every mailpiece as it flows through the system – giving true visibility into the mailstream. Intelligent Mail barcodes, combined with other requirements such as electronic documentation and appointment scheduling, can take your mail and business to new heights.
From This
To This
What are the Intelligent Mail® Barcodes?
Intelligent Mail® Barcode (for Letters and Flats)
Transitional 10/24-Digit Intelligent Mail® Tray Label
24-Digit Intelligent Mail® Tray Label*
Intelligent Mail® Container Label & Barcode
Intelligent Mail® Package Label & Barcode*
SCF SAN FRANCISCO CA
STD FLTS SCF BC/NBC
940
USPS DELIVERY CONFIRMATION
420 12345 9112 3456 7890 1234 5678 9012 34
*Subject to change pending final approval.
What can Intelligent Mail do for your Business?
How your business implements Intelligent Mail determines the benefits received. With Intelligent Mail there are opportunities for your business to:
Experience new and enhanced products and services
Improve contact with customers
Achieve greater accountability and visibility of your mailings
Obtain information to better manage your resources, operating costs and marketing expenses
Improve mailing lists with feedback provided on mail and address quality
Where can I learn more?
Visit ribbs.usps.gov to find out more information on the Intelligent Mail Vision, the Intelligent Mail barcodes, and related service offerings.

Figure 4.3
Intelligent mail advertisement. Image from the USPS.

Mail, however, offers not only a snapshot of mail flow but also of worker behavior. As letter carriers travel through their assigned routes, Intelligent Mail Devices create a digital record of the carrier's behavior. All collected data are stored in the USPS' information backbone, the Intelligent Mail Visibility Service.[79]

Key players from across the postal industry—including bulk commercial mailers such as American Express and Capital One; marketing companies, including ADVO, Acxiom, and Young & Rubicam; catalog and greeting card manufacturers; and communications companies, such as Siebel Systems, Symbol Technologies, and R. R. Donnelley—initially envisioned Intelligent Mail as a way to cater to the needs of large mailers.[80] Intelligent Mail data are used to create a host of value-added services sought by commercial mailers, such as bulk track-and-trace services and advance notification of incoming mail.[81] These services allow commercial mailers to better manage their logistics but offer little to the more general mailing public. In this respect, Intelligent Mail represents the fracturing of the postal network: general users are offered a set of basic services, while sought-after markets—commercial mailers—are provided with enhanced value-added upgrades.[82] Intelligent Mail is an important strategic initiative for USPS. As postal volumes decline, value-added services structured around the commodification of information offer USPS one of the few possibilities of revenue growth.[83]

Intelligent Mail is also critical to the reorganization of labor relations within the postal network. The collection of fine-grained, real-time network data offers the opportunity to shift how labor is deployed.[84] "Total mail visibility" not only enables mailers to peek inside the postal network and track the circulation of their mailings but also generates data tracking postal workers as they travel outside the office. Expanded surveillance is critical to the ongoing expansion of the use of temporary, casual labor. Since the mid-1980s, USPS has prioritized the use of temporary workers as a means of controlling costs. Nonunion, noncareer employees work for lower wages and, in most cases, do not receive the benefits afforded career employees.[85] Intelligent Mail data provide management with the ability to quickly evaluate individual performance, which is increasingly useful when applied to temporary workers, who, unlike career employees, can be added and subtracted from employee rolls with little difficulty. Further, Intelligent Mail enables management to finely calibrate the deployment of temporary workers to meet short-term fluctuations in workload, adjusting staffing levels in response to temporary spikes and depressions in mail volume.[86] Historically, postal labor has been dominated by a highly

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

unionized career workforce, with employees typically occupying stable roles day after day. The move to flexible labor allows management to hire and fire low-cost staff as needed and, importantly, shift workers to meet changing demand. Intelligent Mail, seen within this larger context, appears to be not only a way to create new products but also a part of the larger ongoing reorganization of postal labor.

The positioning of Intelligent Mail as a security technology was an afterthought. USPS and its corporate partners developed it for quite different purposes in response to issues unrelated to security. Yet as Intelligent Mail was being reviewed and considered for adoption, the Postal Service and the industry used the threat of biological terrorism to justify moving forward with the project.[87] The Postal Service argued that Intelligent Mail offered clear security benefits. Real-time processing and distribution data generated through Intelligent Mail could be used to isolate cross-contaminated mail and reroute other mailings away from contaminated sites. Additionally, the wealth of data produced through Intelligent Mail, the Postal Service argued, would assist investigators by allowing them to retroactively trace the movement of contaminated mail through the network.[88] The only real distinction between Intelligent Mail's security features and its commercial and managerial uses relates to how data are used. In the context of debates about postal security, it emerged as a possible new "fix" that could complement the BDS.[89] The same qualities that make the collection of real-time postal data attractive as a commodity and operational tool—increased customization, visibility, and control—make it a useful security instrument.

Although "security" offered a rationale for the adoption of Intelligent Mail, it is important to see the program as a key element of a larger transformation of the Postal Service. The shifts that Intelligent Mail enables—toward boutique, customized products tailored to commercial mailers and toward a greater reliance on temporary workers—are not value neutral. Intelligent Mail, like the BDS, is inscribed with a certain politics. The remaking of the Postal Service into a flexible, informational enterprise benefits particular users and categories of workers at the expense of others. With Intelligent Mail, the Postal Service moves away from offering uniform services that are available to all customers and embraces new product lines that cater to the needs of commercial mailers. Intelligent Mail, like the BDS, prioritizes bulk mailers over small-scale or individual mailers. At the same time, Intelligent Mail undergirds the ongoing transformation of postal labor: it supports the replacement of career workers with low-cost, temporary workers.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The Sunk Politics of Biohazard Security

The 2001 anthrax attacks illustrate both the power risks to destabilize the gridlock of politics as usual and the limitations of these moments of fissure. The attacks did not conform to the established narratives of how an anthrax attack would unfold and undermined long-standing biodefense efforts. In this moment of post-9/11 disruption, the new efficiencies enabled through regulatory reform were reframed: centralized processing and the adoption of automation—the successes of the transformation of the governance of the postal system during the 1970s and 1980s—became acute problems. The newly created MSTF reversed, if only for a moment, the organization of power within the postal system. It brought together, in a deliberative setting, labor, mailers, management, and relevant experts to discuss how to confront the crosscutting challenges of postal security. In this sense the anthrax attacks were a catalyst for a new mode of inclusive postal politics. For decades, mailers have largely steered postal decision-making through formal and informal linkages to postal management, while labor has been marginalized. Here, the attacks appear to illustrate the political potential of novel risks to spark inversion and new political formations.

The catalytic potential of the anthrax attacks to upend hierarchies of power was, ultimately, qualified and temporary. Opening the black box of security standards reveals the reentrenchment of old hierarchies of power. The assemblage of technologies designed to counter the threat of biological terrorism are not apolitical or neutral: they privilege certain forms of use over others, distribute costs unequally across different categories of users, prioritize commercial concerns over worker safety, and engage in the policing of labor to aid the shift toward temporary workers. In this manner, these new security interventions are consistent with the larger trajectory of deregulation. In the cases of freight rail and electric power, however, the outcomes would be different. As the following pages detail, in these infrastructures fears over terrorism would lead to significant and lasting changes that reordered power. New regulations would impose new forms of accountability that directly challenged the material and social changes unleashed through deregulation. These changes would not arrive without a fight.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

5

Green Security: The Environmental Movement, the Transportation of Hazardous Materials, and the War on Terror

The current state of our rail security system is worse than an accident waiting to happen, it is an open invitation to terrorists. We need to close these loopholes before terrorists exploit them. I don't want to read a blue ribbon commission report telling us steps we could have taken. Common sense tells us we must act now.
—Senator Joe Biden, June 16, 2005[1]

On September 13, 2005, 50 protesters lay silently in front of the U.S. Capitol building as a man dressed in a hazmat suit surveyed the field of mock fatalities. In the background, a 40-by-12 replica railroad tank car emitted smoke and a persistent hiss. Painted on the outside of the car and reproduced on shirts worn by the protesters was the slogan "Reroute [and] Phase-Out Chemicals of Mass Destruction" (see figure 5.1). The tableau was intended to represent the aftermath of a terrorist attack targeting a 90-ton railcar filled with dangerous chemicals. Greenpeace had staged this act of theater to highlight the federal government's failure to enact legislation or regulations protecting the transportation of hazardous materials from terrorist attack. As Greenpeace legislative director Rich Hind noted, the simulation was designed to force Congress to imagine the effects of a real chemical disaster.[2] In an odd twist on post-9/11 politics, environmentalists argued that the Bush administration was too lax in its engagement in the war on terror; in their estimation, the government was largely ignoring the threat of terrorism.

Since 9/11, the rail industry has faced a crisis of control. Rail shipments of large quantities of hazardous materials passing near or through urban areas offer terrorists an inviting target. As the Association of American Railroads notes, "chemicals and rail transportation go hand in hand."[3] The chemical industry is a key rail customer. Chemicals account for a significant share of *all* rail traffic. In 2018, railroads hauled 2.2 million carloads and over 181 million tons of chemicals (7.4% of all carloads

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

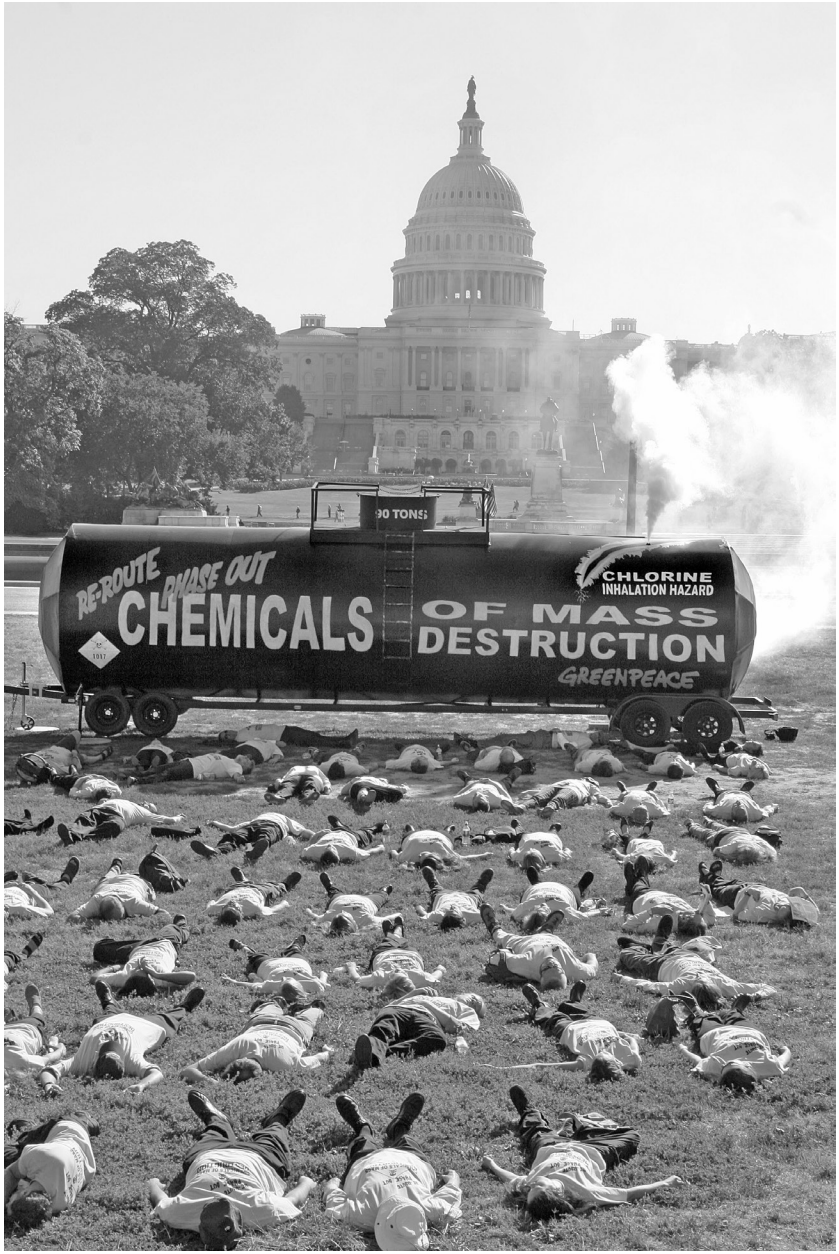


Figure 5.1
Toxic train accident demonstration on the West Lawn, U.S. Capitol, September 13, 2005. Image copyright Rick Reinhard/Greenpeace.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and 11% of total tonnage). These chemical shipments accounted for $11 billion in rail revenue—14.5% of all rail revenue for the year.[4] Chemicals were the second largest source of revenue by product category for railroads; and second in terms of sheer tonnage behind only coal.[5] These dangerous materials travel across a domestic rail network that is largely open, unsupervised, and often operating close to cities.[6] An attack targeting a large shipment of particularly hazardous chemicals could have dramatic results. In widely quoted testimony not long after 9/11, Dr. Jay Boris of the Naval Research Lab detailed that an attack on an 90-ton railcar carrying chlorine could, under the right circumstances, kill 100,000 people in a densely packed urban area in as little as 30 minutes.[7] Post-9/11, rail cargoes of hazardous materials were reframed, in the words of then senator Joe Biden, as "rolling weapons of mass destruction."[8] Federal law, regulations, and voluntary industry practices have historically been preoccupied with rail "safety" and were pitched to prevent and mitigate unintentional accidents. After 9/11, however, security became a new and pressing concern. Calls for the introduction of tighter security measures to confront the threat of terrorism came from many corners; the environmental movement, local and state officials, members of Congress, and the rail industry each advocated for enhanced rail security for hazardous materials. What form such new measures would take, however, was an open question. Though a near consensus existed that the pre-9/11 status quo on rail safety needed rethinking and remaking, what direction such reforms should take was deeply, and at times bitterly, contested.

* * * *

This chapter examines the post-9/11 battle over the shipment of hazardous materials. Environmental groups, such as Greenpeace, the Sierra Club, and Friends of the Earth, advocated for strict new security regulations concerning the routing of hazardous materials shipments. Pointing toward the threat of terrorism, these groups backed local city councils and state governments, as well as some prominent federal legislators, in seeking to enact strict security regulations directing railroads to reroute hazardous cargoes away from urban areas. The perceived risk of terrorism provided a new way of building a political coalition to advocate change. Environmental activists fought for rerouting not only as a way to reduce the risks associated with transporting hazardous cargoes close to cities but also as an indirect means of achieving their long-standing goal of limiting the use of toxic materials, particularly chlorine, in industrial production.[9] By limiting flows of toxic materials via routing restrictions, environmental activists

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

sought (and seek) to make it more difficult to access industrial chemicals and encourage the adoption of safer substitutes.[10]

This coalition went up against the might of both the rail and chemical lobbies. The rail and chemical industries pushed back against post-9/11 calls for routing controls.[11] The chemical industry plainly rejected rerouting on the grounds that it added costs and limited the availability of its products.[12] Transportation regulations, in their view, were something of a backdoor way to ban or otherwise threaten the market for chemicals. The railroads' objections were slightly more nuanced. Railroads sought to maintain their hard-won autonomy to determine the material flows of their networks and utilize the most profitable shipping routes. Deregulation had freed railroads to shed unprofitable track and to select routes of their own choosing. Rerouting, potentially, would jeopardize this autonomy.

Common-carrier obligations require railroads to haul hazardous materials, whether they wanted to or not.[13] Although chemicals are a large revenue source for railroads, there is comparatively little money to be had in transporting the most dangerous materials. Post-9/11 rerouting debates focused on a particularly dangerous subset of hazardous materials, toxic-inhalation-hazard (TIH) materials. TIH accounts for a tiny fraction of total rail cargo.[14] But mandatory rerouting targeting TIH *does* threaten rail profitability. TIH materials, like most other hazardous cargoes, often travel as part of manifest trains transporting all types of other cargo (that is, they do not only travel independently on dedicated trains).[15] Rerouting even a fraction of chemical shipments would require rerouting all of the other commodities on board the assembled train. Railroads would have been perfectly happy to refuse to carry TIH materials and see their common-carrier obligations—one of the last remaining vestiges of the old model of regulation—relaxed. But if they had to carry these chemicals, they wanted to do it on their own terms. Ultimately, the railroads joined the chemical lobby to fight mandatory regulations.[16]

Arguments over rail hazmat security were an oblique referendum on deregulation. Debates considered a range of possible remedies and mitigation measures, including improved tank car design, the introduction of positive train control (PTC), the adoption of inherently safer technologies (ISTs), and stricter personnel controls for rail employees. Rerouting was the most divisive issue—the antagonisms at play between various infrastructure publics, including local and federal government, activists, and industry, were (and are) sharply defined. Arguments over rerouting wrestled with the legacy of deregulation. During the late 1970s and 1980s, deregulation revitalized freight railroads and pulled the industry from the brink of ruin

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

(see chapter 2). Deregulation transformed power within the rail industry: it provided railroads with far greater autonomy over rail operations while limiting public oversight in significant ways. Regulatory reform also transformed the material rail network. It made it much more efficient while also increasing the flow of large shipments of hazardous cargo across a shorn and lean rail network. In a real sense, this meant that more frequent shipments of large batches of hazardous chemicals now traveled on routes near (or through) large cities. As in the other surveyed infrastructures, deregulation promoted the development of efficient networks at the expense of increasing large-scale vulnerability. The debate on rerouting confronts and struggles with this legacy as it considers the limits of the railroads' power and the role that other infrastructure publics play in rail policy.

From Safety to Security: Hazardous Materials Regulation in Historical Perspective

Immediately after 9/11, public officials looked toward the transportation of hazardous materials as a terrorist target. Richard Falkenrath, former deputy Homeland Security advisor to President Bush, observed in testimony before Congress that "of all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive and susceptible to terrorist attack: toxic-inhalation-hazard industrial chemicals."[17] New laws, regulations, and voluntary practices expanded the scope of traditional rail safety measures to include an emphasis on rail security. The movement from "safety" to "security" was a significant shift. It was part of the larger reordering of infrastructure as "dangerous things" that was afoot. Taking seriously the possibility of intentional disruptions and attacks, not just accidents, resulted in the creation of a new agency—the Transportation Security Administration (TSA)—and the enlargement of the regulatory responsibilities and purview of the Department of Transportation (DOT). Also, as part of this initial recalibration toward rail security, the Association of American Railroads (AAR), the largest rail industry trade association, introduced new voluntary security measures covering the handling of hazardous materials.

The focus on security was transformative. Historically, the mix of federal legislation, regulations, and industry voluntary practices that had governed the transportation of hazardous materials focused on safety. These rules and practices were structured to counter accidents and had largely ignored the possibility of intentional disruptions. Voluntary regulation of hazardous materials began in 1907 with the creation of the Bureau of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Explosives by the American Railway Association (ARA), an industry trade association.[18] In the following year, at the behest of the ARA, Congress passed legislation providing the Interstate Commerce Commission (ICC) with the authority to regulate shipments of hazardous materials. The ICC promptly granted the Bureau of Explosives power to develop and enforce hazardous materials regulations covering explosives and a wide range of other hazardous cargoes.[19] The Bureau of Explosives created regulations concerning labeling, handling, and container specifications and performed periodic inspections.[20] In 1966, the ICC's authority to regulate hazmat transportation was shifted to DOT.[21] Subsequently, the Federal Railroad Safety Act, the Hazardous Materials Transportation Control Act of 1970, and the Hazardous Materials Transportation Act of 1975 consolidated the authority of DOT and provided the modern legislative authority for the regulation of rail safety and hazardous materials transportation.[22] Contained in Title 49 of the Code of Federal Regulations (49 C.F.R), DOT developed complex regulations governing the packing, handling, labeling, and designation of hazardous materials.[23] Further, DOT developed engineering standards for tank cars and hazmat containers and possessed the authority to levy penalties for noncompliance. Within DOT, the Research and Special Programs Administration (RSPA) took responsibility for developing hazmat regulations while the Federal Railroad Administration (FRA) enforced regulations.[24] The AAR, the successor to the ARA, developed voluntary standards and conducted inspections complementing federal standards.[25] All of these efforts were, in the main, focused on safety—the prevention of accidents involving hazardous materials.

To a large degree, this assemblage of regulations and voluntary practices worked quite well; as AAR highlights, 99.99% of all rail hazmat shipments reach their destination without incident.[26] Between 1980 and the early 2000s, rail accidents decreased by 75%, and accidents involving releases of hazardous materials declined by 91%.[27] Although the adoption of a more narrow definition of what constitutes a reportable hazmat accident in the early 1980s slightly inflates the degree of improvement, routine rail shipments of hazardous materials are generally safe, and accidental releases are rare.[28]

In the wake of 9/11, however, the possibility of a terrorist attack on rail shipments of hazardous materials became an area of public concern. Previously, when security was considered at all, concerns were limited to unauthorized access to rail facilities by trespassers and vandals. Authorities primarily fretted over accidents—and the resulting liability—caused by the use of rail facilities by recreational motorsports enthusiasts (what

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

is known as the "ATV problem") and trespassing.[29] After 9/11, however, rail security took on a new meaning and became viewed through the prism of terrorism: top public officials openly speculated about the possibility that terrorists might target large shipments of toxic materials, particularly TIH materials, such as chlorine, in order to cause mass casualties in the U.S. As with other systems, the threat of terrorism became part of the taken-for-granted background against which arguments over infrastructure policy were made. The perceived threat of terrorism introduced a new, salient uncertainty into rail operations.[30] Safety measures designed to confront rail accidents, or relatively minor incidents of unauthorized access, were quickly viewed with scorn: measures that were perhaps fine for managing the "ATV problem" began to look ill-suited for confronting international terrorism.

The shift toward security was consequential. As concern turned away from accidents and toward intentional acts of sabotage, the accumulated safety record of railroads in transporting hazardous materials suddenly became, if not moot, somewhat incidental to the debate. If the terrorist threat represented something new—an evolving hazard just emerging—then historical data were of little guidance. Fairly rigorous data on rail accidents and hazmat incidents had been collected for decades. From this data, accident probabilities had been derived with a degree of confidence. However, when a new hazard—terrorism—was added to the equation, the historical record no longer provided a clear glimpse of the future. There was no guarantee that the future would mimic the past. In this gulf, imagined possibilities started to replace calculated probabilities: fantasy worst-case scenarios became legitimate points of reference.[31] As debates over rail security gained steam and grew increasingly contentious, recent accidents involving hazmat cargoes became portentous. Advocates for stricter measures pointed toward recent accidents—including in Minot, North Dakota; Graniteville, South Carolina; and Baltimore—to emphasize the danger of hazmat shipments while noting that the destruction from these accidents would pale in comparison to a targeted attack.[32]

Rethinking Rail Security after 9/11: Preparing for a "Big Bang"

Initial industry and federal action to address security concerns commenced shortly after 9/11. At the start of the war in Afghanistan on October 7, 2001, all rail shipments of hazardous materials within the U.S. were suspended for 72 hours out of fear of sabotage.[33] The rail industry, through AAR, quickly formed a security task force to review and offer

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

recommendations on hazmat transportation.[34] At the federal level, Senator Jon Corzine introduced the Chemical Security Act of 2001 on October 31, 2001. The bill sought to address the threat of terrorism to chemical facilities and carriers of large quantities of chemicals. The proposed legislation would have given the Environmental Protection Agency authority to mandate tighter security regulations of facilities producing or storing certain chemicals and promote eliminating the transportation of such chemicals.[35] Paul Orum, director of Working Group on Community-Right-to-Know, singled out the chemical and rail industries for criticism in comments in a November 12, 2001, *Washington Post* story highlighting gaps in chemical facility and hazmat transportation security.[36] Orum charged that "industry has been in denial about the need to reduce those hazards and set measurable goals and time lines." [37] Frank Webber, president of the American Chemistry Council, an industry lobbying group that counted DuPont, Dow, and other companies in its ranks, conceded that a terrorist attack targeting large stocks of chemicals was a possibility.[38] Webber was blunt telling the press that "no one needed to convince us that [the chemical industry] could be—and indeed would be—a target at some future date."[39] He noted that if terrorists were "looking for the big bang, obviously you don't have to go far in your imagination to think about what the possibilities are."[40] But, despite these admissions, Webber and the chemical lobby argued that there was no need for new legislation. Industry, they assured, was already hard at work addressing the issue.[41] Corzine's bill faced stiff opposition and stalled. The Aviation and Transportation Security Act, enacted November 19, 2001, however, created TSA within DOT and tasked TSA with overseeing new security procedures across all modes of transportation, including freight rail.[42] TSA, however, initially focused almost exclusively on aviation security.

The rail industry sought to address the issue through voluntary measure. In December, AAR implemented security controls as part of its newly created Terrorism Risk Analysis and Security Management Plan.[43] As part of this plan, AAR created the Railway Alert Network to share information between railroads and intelligence agencies relating to credible threats and security issues. DOT issued an advisory notice in February 2002 echoing AAR's voluntary measures and encouraged railroads to review their security plans—including background checks and en route and facility security.[44] Though there was a brief spike in interest by industry and the federal government in rail security in the months immediately following 9/11, without specific threats or an attack directed toward rail—or significant interest group pressure—attention and action tapered off.[45] It appeared that, as in

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the case of the postal system, industry would be able to control and dictate how new forms of infrastructure security would unfold.

The Homeland Security Act of 2002 and HM-232

Rail security was again thrust to the fore in 2002 as the FBI issued a public warning and environmental activists pressed the issue. In October the FBI provided the first specific warning to law enforcement, rail companies, and the public indicating that Al-Qaeda was targeting U.S. rail shipments of hazardous materials.[46] The FBI alert sourced the warning from information gleaned from captured detainees. Previously, concerns over rail security and terrorism had been substantiated only through inference. Now, for the first time, the FBI stated in public that railroads and shipments of hazardous materials in the U.S. were targets of terrorist action. The FBI warning offered an opening: Greenpeace, Friends of the Earth, and the Sierra Club pushed the issue of hazmat transportation security. The use and transportation of hazardous chemicals had been a long-standing issue of concern and activism for environmentalists; environmental groups—legitimized by warnings from the FBI—now invoked the threat of terrorism in calling for greater public controls over toxic cargoes.[47] Activists appropriated the language of national security in order to advance their claims; they acted as "risk entrepreneurs" by seizing on the availability and salience of fears of terrorism to forward their arguments and forge new political coalitions. Environmental groups supported Senator Corzine's introduction of chemical security legislation again in 2002 and pushed for more extensive controls than the voluntary actions taken by the railroads. Environmental groups' legislative agenda rested on two main goals: support for rerouting toxic shipments away from cities and support for inherently safer technologies that would reduce or eliminate the reliance on toxic chemicals in manufacturing (which would, in the process, eliminate the risks associated with the transportation of such materials).[48]

Although the Corzine legislation again failed to advance, new legislation and modest regulations touching on hazmat transportation security did move forward. The Homeland Security Act of 2002 created DHS and moved TSA under DHS authority (see chapter 3). Importantly, the Homeland Security Act also amended portions of Title 49 of the U.S. Code relating to the scope of DOT's power. The Homeland Security Act enlarged the responsibility of DOT to include rail and hazmat *security* in addition to safety.[49] This created a new set of authorities and regulatory powers for DOT. Despite shifting TSA to the newly created DHS, the act explicitly delineated rail security and hazmat transportation security as

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

areas that would remain firmly within DOT's authority. DOT now had a mandate to address security and the expanded power to do so.

Despite this broad new mandate, DOT was cautious. The first set of regulations introduced under the new powers granted by the Homeland Security Act continued the industry's preference for lax, mostly voluntary measures. The regulations did little to alter power within the rail industry or change how rail companies operated. The new regulations, known as HM-232, acknowledged the danger represented by rail shipments of hazardous cargo near urban areas but exhibited great deference to rail industry prerogatives. In the publication of the Final Rule, DOT noted that "the September 11th terrorist atrocities to [*sic*] indicate the heightened risk of terrorism with which we all now live and the need to reassess and address security vulnerabilities in all areas of our public and private lives."[50] Further, DOT recognized that the threat of terrorism required adapting hazmat regulations to the unique challenges of intentional disruption. Nonetheless, HM-232 only placed loose requirements on rail carriers of select hazardous cargoes to draft and file a security plan and increase training for workers.[51] Under the new rules, security plans were required to be in writing and, at minimum, had to address en route security, personnel practices (i.e., hiring practices and background checks), and unauthorized access.[52] Crucially, the regulations did not identify any specific measures to be taken or require railroads to address the routing of hazardous materials through or near large population centers. While the regulations required the development of a security plan, what form such a plan took, or how (if at all) it was to be put into action, was left largely to the discretion of each individual railroad.

Environmental groups were dissatisfied with HM-232. They had hoped that under the sign of security, DOT might introduce new strict rules governing the transportation of dangerous materials.[53] Yet the first set of regulations largely left substantive decisions concerning rail security in the hands of the industry.[54] The enlargement of the scope of DOT's powers provided the nascent possibility of revisiting and ultimately revising how toxic materials flowed through the rail network. Once on the books, these new powers could be put in service of different uses. However, at first pass the rail industry and the chemical industry won victories that did little to alter the status quo: new regulations left the private sector with the ability to decide through which routes hazardous materials moved. Yet, taken as a whole, this early action on hazmat security was not entirely inconsequential. By adopting legislation giving DOT clear power to act on issues of rail hazmat security, the possibility remained that new, more

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

stringent regulations could possibly be introduced at a later date. After the disappointment of the new DOT regulations, environmental activists turned their attention and efforts to a new avenue: the pursuit of city and state rerouting legislation.

Risk Coalitions: Rerouting, Preemption, and the War on Terror

If the federal government would not take hazmat transportation security seriously, perhaps cities and states would? While rerouting legislation stalled in Congress and the first set of new regulations proved a disappointment, environmental groups pursued local and statewide measures to mandate the rerouting of toxic materials away from urban areas. The aim of this strategy was twofold: the piecemeal pursuit of local controls could, in aggregate, limit the shipment of hazmat cargoes near dense population centers, and more importantly, the passage of legislation could force the federal government to enact meaningful rerouting rules. With the support of Greenpeace, Friends of the Earth, and the Sierra Club, at least 14 different cities and states—including Washington, DC, Boston, Cleveland, Chicago, Buffalo, Saint Louis, Memphis, Las Vegas, and the state of California—considered rerouting legislation.[55] Reframing the risks of hazardous materials transportation as an issue of terrorism, rather than a purely environmental concern, helped forge new coalitions and press action. The larger post-9/11 cultural and institutional redefinition of infrastructures as dangerous things was, at this point, well under way (see chapter 3). These changes made it possible for organized interests (environmental activists and their allies) to reframe hazmat transportation as an issue of national security—even the chemical lobby agreed that chemical shipments were a terrorist target—and have their arguments appear legible and gain traction. The local strategy paid dividends: Washington, DC, passed the first local ban in 2005.

The Terrorism Prevention in Hazardous Materials Transportation Emergency Act of 2005

Washington, DC, offered an attractive test case. The city's role as the nation's capital, its symbolic significance, and its recent history—the 9/11 attacks targeted the city, as did the anthrax attacks—made it easy to argue that the city was a potential terrorist target.[56] Additionally, CSX, one of the largest U.S. railroad companies, operated two rail lines that transported hazardous materials through the city: the "I-95 line," the north–south main line stretching from New England to Florida, and the "B&O" east–west

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

main line connecting with Chicago and Saint Louis.[57] CSX shipments of 90-ton chlorine tank cars ran a mere four blocks from the U.S. Capitol, well within the range of exposure from an intentional or accidental release.[58]

The DC City Council first considered a local ban on rail shipments of certain hazardous materials in 2003. After introducing legislation in 2003 and again in 2004, the DC City Council agreed to table any action while DOT formulated comprehensive new security regulations.[59] They agreed to wait and see what DOT came up with. Federal regulators had stated that HM-232, DOT's initial set of regulations, was just a first step. A larger overhaul, they said, including a new stricter regulatory framework for hazmat transportation was in the works.[60] Yet, after waiting in vain for two years, DOT had not made any real progress. They had not issued (or even hinted at) new comprehensive regulations. The DC City Council, led by Councilwoman Kathy Patterson, had waited long enough. They decided to act. They viewed the lack of a thoroughgoing federal action to be an abdication of responsibility. Patterson noted that despite the "massive danger" of a terrorist attack targeting large shipments of dangerous materials, since 9/11 "no enforceable or regulatory action has been taken by the Federal Government to eliminate this threat."[61] Councilwoman Patterson introduced the Terrorism Prevention in Hazardous Materials Transportation Emergency Act of 2005 on January 28, 2005. On February 1, the DC City Council voted 10–1 in support; two weeks later, on February 15, Mayor Anthony Williams signed the act into law, making Washington, DC, the first city to enact a local ban on shipping hazardous materials by rail.[62]

The DC Council succinctly stated the case for mandatory rerouting. In legislative findings accompanying the act, they noted that the unique position of DC as a center of American politics and history made it an inviting terrorist target and that "a terrorist attack on a large-quantity hazardous material shipment near the United States Capitol … would be expected to cause tens of thousands of deaths and a catastrophic economic impact of $5 billion or more."[63] Further, the act was explicitly designed to underscore federal inaction, as the DC Council stated: "The federal government has not acted to prevent the terrorist threat resulting from the transportation of dangerous quantities of ultrahazardous materials near the Capitol."[64] The deferential regulations contained in HM-232, coupled with the unfulfilled promise by federal regulators to follow up with tighter regulations, rung hollow for the DC Council.[65] If DOT would not act, the city council would.

The act prohibited shipments of large quantities of explosives, flammable gases, or TIH materials within a designated 2.2 mi. radius of the capital,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

known as the Capital Exclusion Zone. The act did, however, contain possible exceptions: it allowed shipments during emergencies and authorized the DC Department of Transportation to issue permits allowing transport if no alternative route existed or if such routes were determined to be cost-prohibitive.[66] The act was plainly directed at CSX: its main north–south and east–west lines both fell within the Capital Exclusion Zone.[67] The intent behind the act was to force CSX to enter into interchange agreements with other railroads to reroute specified cargoes across nonurban lines and limit the shipment of hazardous materials through the city.[68]

***Legal Challenge:* CSX v. Williams**

The rail industry did not take long to respond. On February 16, 2005, the day after Mayor Williams signed the act into law, CSX filed suit in the U.S. District Court for the District of Columbia, seeking a permanent or temporary injunction to block the act before it could take effect.[69] The case pitted the federal government, the railroads, and the chemical lobby against a coalition of environmental activists and municipal and state governments. These various publics were fighting over the power to control infrastructure. The case was in direct dialogue with deregulation: it implicitly and explicitly questioned the compatibility of the market with security; it suggested that efficiency, in some ways, was not the sine qua non of public policy and that other concerns also mattered; and it sought to roll back the autonomy of the railroads and enhance new public controls over their operation. The Department of Justice argued in support of CSX, while the Sierra Club joined Washington, DC, in arguing in support of the act before the district court and on appeal in the U.S. Court of Appeals for the District of Columbia. Heavy hitters from the rail and chemical industry lined up behind CSX. AAR, Norfolk Southern (a major rail company), the National Industrial Transportation League (an industry trade group), the American Chemistry Council (the lobbying arm of the chemical industry), and others joined CSX as amici curiae.[70]

The case took a slightly new look at a familiar question: What role, if any, could local communities—cities and states—have in regulating national infrastructure? This question sat at the heart of the late-19th-century debates and battles over the power of railroads (see chapter 1). The Supreme Court struck a stake through state regulation of interstate rail rates and limited the role that state and local governments could play in *Wabash v. Illinois* (1886).[71] After *Wabash,* the federal government, and not states or municipalities, would play the decisive role in regulating the railroads. This case revisited these old debates within a decidedly new context. In the words of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

presiding District Court Judge Emmet G. Sullivan, the case involved "the longstanding principles of federalism applied to one of the government's newest and most important roles—protecting our Nation from threat of terrorism."[72] The case asked: What, if any, role should local communities have in crafting ordinances to combat terrorism? Specifically, could the District of Columbia, "pursuant to its traditional police power … prohibit the rail carriage of certain hazardous materials"?[73] Or does federal law take precedent and prevent enforcement of the act? The precise legal question in the case turned on the limits of federal preemption of local law.[74]

CSX clearly saw the larger stakes. This case was about much more than the Capital Exclusion Zone. CSX claimed that the DC act would open the door for copycat local legislation that could cripple the nation's interstate rail system.[75] CSX argued that the act: (1) violated the Commerce Clause of the Constitution; (2) was preempted by the Federal Rail Safety Act, the Hazardous Materials Transportation Act, and the Interstate Commerce Commission Termination Act; and (3) was at odds with the legislative authority given to Washington, DC, under the Home Rule Act.[76] The question of preemption was central to both the district court ruling and the eventual ruling by the U.S. Court of Appeals for the District of Columbia. The Federal Rail Safety Act and the Hazardous Materials Transportation Act each contain language indicating that federal law preempts—that is, takes precedent over—local and state legislation under certain conditions. The purpose of preemption, as spelled out under the amended Federal Rail Safety Act, is to ensure that "laws, regulations, and orders related to railroad safety and laws, regulations, and orders related to railroad security shall be nationally uniform to the extent practicable."[77] The Homeland Security Act of 2002 explicitly retains the preemption provisions of both the Federal Rail Safety Act and the Hazardous Materials Transportation Act.[78]

The preemption provisions in question are not airtight. Under certain circumstances, local jurisdictions *can* enact more strict rules and regulations. The Federal Rail Safety Act allows states to regulate rail safety and security "until" the federal government "prescribes a regulation or issues an order covering the subject matter of the State requirement."[79] If the federal government has yet to act in a specific area of rail security or safety, states can act. The Federal Rail Safety Act further creates a safe harbor for states to act *even if* the federal government has acted if the state law, regulation, or order: "(1) is necessary to eliminate or reduce an essentially local safety or security hazard; (2) is not incompatible with a law, regulation, or order of the United States government; and (3) does

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

not unreasonably burden interstate commerce."[80] The preemption provisions contained in the Hazardous Materials Transportation Act echo the Federal Rail Safety Act and preempt state law when it is not possible to comply with both state and federal regulation or if state regulation creates a barrier to compliance with federal regulation.[81]

In examining the DC act, the courts looked at two basic questions: (1) Has the federal government already acted on the topic covered within the DC act? (2) If so, does the DC act fall within allowable safe harbor provisions? The stakes were clear. If the federal government was found to not yet have acted, then the DC rerouting ban would likely rest on firm legal ground. Additionally, even if the federal government had already acted, the DC ban could survive if it was found to address a local hazard in a manner that is not at odds with federal regulation or burdens interstate commerce.

CSX v. Williams*: U.S. District Court, District of Columbia*

The DC city council scored an initial victory. The district court denied CSX's motion seeking a preliminary injunction preventing the enforcement of the DC act. The law would take effect as a full proceeding considered the status of a permanent injunction.[82] In examining new federal regulatory efforts, the district court identified a gap in federal regulations that left open the door for state rerouting. The court noted that rail hazmat security is, essentially, a new task that stands outside traditional safety regulations.[83] For the district court, the threat of terrorism presented a new hazard and challenge to rail operations. In this regard, existing regulations directed toward the routine operational risks of transporting hazardous materials were seen as distinct from regulations that focused on the deliberate targeting of hazardous cargoes by terrorists. In other words, safety and security were taken to be different. Security, in the court's view, was a new domain. When the court turned to review current federal efforts touching on this topic, it found little evidence of any regulatory action.[84] The court was dismissive of DOT's current regulation, HM-232.[85] The court refused to accept that the call to develop basically voluntary security plans could serve to preempt the DC act.[86] It noted that the text of HM-232 identifies that regulation as merely a partial first step and that comprehensive and authoritative federal hazmat transportation security regulations would be forthcoming.[87] Here, the court found a gap in federal action that would allow states to act: until further comprehensive and authoritative federal regulations covering the security of rail shipments of hazardous cargoes were introduced, states and cities were free to introduce legislation.[88]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The district court also examined whether the DC act prevented compliance with current federal regulations. Here again the court considered HM-232. The court found no reason why CSX could not comply with HM-232's general requirement to craft a security plan *and* abide by the DC act's requirement to reroute hazardous cargo away from the Capital Exclusion Zone. In the court's view, these two approaches were compatible. CSX and the Department of Justice pushed back. They argued that HM-232 was explicitly designed to provide railroads with the flexibility to craft security plans tailored to their unique circumstances. In their view, by requiring rerouting, the DC act hindered this flexibility. As a result, DOJ and CSX argued, the local rules stood in conflict with existing federal regulations. The court was not moved. In a blow to CSX and the rail industry more generally, the DC measure was allowed to stand as a gap-filling measure.[89] A permanent injunction could still be considered by the court, but the door to local regulation had now, at least for a moment, been wedged open.

CSX v. Williams*: U.S. Court of Appeals*

CSX and DOJ appealed the district court decision and sought an emergency injunction to block the DC act.[90] CSX filed an emergency motion with the court of appeals on the same day that the district court's ruling was issued. The court of appeals heard the case a little over a week later. In reviewing the district court's ruling, the court of appeals again examined the questions of preemption and HM-232. The court of appeals broke with the district court. It asserted that the toothless voluntary regulations in HM-232 *did* qualify as federal action. The preemption provision of the Federal Rail Safety Act allows the court only to determine if the regulation covers the subject matter, not to gauge its relative effectiveness.[91] The court of appeals noted that DOT had originally considered more stringent rerouting measures but ultimately settled on the voluntary approach. Regardless of whether this remedy was imperfect, in the court of appeals' view HM-232 was a federal action on rail hazmat security. While the district court placed considerable weight on the notion that HM-232 was presented as the first in a succession of comprehensive rules that had not yet materialized, the court of appeals took a narrower view. It simply examined whether there had been *any* form of federal action. The court reasoned that the DC Council's complaint was not that the federal government had failed to act but that it had not acted in the manner or to the degree requested.[92] In this reading, the DC act did not qualify as state action designed to fill an unattended gap in federal policy.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The news was not much better for DC and its allies on the safe harbor question. The court of appeals considered whether the DC act fell into the narrow carve-out provided in the Federal Rail Safety Act that allows states to regulate uniquely local hazards. To this end, the court examined whether the DC act (1) was necessary to reduce a local security hazard; (2) conflicted with a law, regulation, or order of the United States government; and (3) placed an unreasonable burden on interstate commerce. The court of appeals determined it likely that the DC act failed to satisfy these three conditions.[93] Terrorism, for the court of appeals, was a national—and not a local—problem. It was, in its reasoning, motivated by a hatred of the United States as a nation.[94] The exception for local hazards were only designed for situations that uniform national standards could not address and in which local communities were uniquely positioned to act.[95] For the court, federal policy could—and indeed had in HM-232—address the security of hazardous rail cargoes. Next, the court asserted that HM-232 was incompatible with the DC act. The preference articulated in HM-232 for voluntary measures was, in the court's view, at odds with the requirement to reroute. The Capital Exclusion Zone would have limited the discretion expressly authorized under HM-232: it would have required railroads to incorporate rerouting around DC as part of their security plans. The district court and the court of appeals saw different balances between autonomy and potential compliance: for the district court, it was possible and reasonable that a railroad's security plan could accommodate rerouting requirements imposed by the DC act and still retain the flexibility outlined in federal regulations; for the court of appeals, the DC act and HM-232 were in clear conflict—the DC act would plainly limit the discretion codified under federal regulations.[96] Finally, the court connected the act to substantial burdens to interstate commerce. The act was model legislation that if allowed to stand would likely have been replicated by cities and states across the county (indeed, this was precisely the hope of activists). The cumulative effect of a number of such local statutes would have severely disrupted the interstate trade in hazardous materials.[97] As the court noted, this was an important test case. If left to stand, surely other cities and states would soon follow DC's lead. As the court noted, the California Senate was considering a bill that would limit hazardous shipments within three miles of any city with a population of over 50,000.[98] As such, the court determined that the DC act did not fall into the safe harbor conditions outlined by the Federal Rail Safety Act.[99]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The court of appeals reversed the district court's ruling and ordered the court to issue a temporary injunction blocking the DC act. It was a serious blow to Washington, DC, and the environmental movement, but it was not the final word on rerouting. The possibility of a permanent, rather than temporary, injunction was still alive (even if its prospects were now grim). The ongoing legal uncertainty surrounding the act, however, pushed DOT to propose new rail security regulations. For activists, the pursuit of local rerouting laws had not been fruitless: it sparked renewed action at the federal level.

Federal Rerouting: Accountability and Infrastructure Reordering

The ongoing litigation over the DC act spurred the introduction of new federal regulations that offered important concessions to those seeking rerouting. The regulations fell between the loose voluntary regulations of HM-232 and the more prescriptive regulations put forward in the DC act and sought by environmental groups. Importantly, as these new regulations were winding their way through the federal bureaucracy, new federal legislation—the Implementing Recommendations of the 9/11 Commissions Act of 2007—would be enacted.[100] This legislation went even further than the draft regulations: it included key provisions sought by environmentalists over the objections of the rail industry. It was an important victory for the environmental movement and their allies.

After the court of appeals granted a temporary injunction against the DC act, the district court began proceedings on a permanent injunction.[101] Though CSX and DOJ had won an important victory in securing the temporary injunction, the case was not yet fully adjudicated. Further, as made clear in the district court's initial ruling, presiding judge Emmet G. Sullivan appeared to be sympathetic to DC and the Sierra Club's arguments in support of local rerouting. Against this backdrop of legal limbo and uncertainty, DOT introduced new federal regulations governing how railroads select routes when transporting hazardous cargoes.[102] The DOT regulations sought to remove any ambiguity concerning the ability of cities and states to enact local rerouting requirements. As the district court had initially found, DOT had promised in introducing HM-232 that additional regulations would be forthcoming. The relative lack of subsequent action, in the district court's estimation, had created a gap in federal regulation that opened the door for states and cities to introduce mandatory rerouting regulations.[103] With the new set of regulations, DOT sought to make it perfectly clear that federal regulations preempted the DC act as well as similar legislative efforts in the works in various cities and states.[104]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA), the successor to the RSPA, which had previously taken the lead in developing regulations, proposed new regulations directing railroads to conduct periodic reviews of routes used to ship hazardous materials and examine the viability of alternate routes.[105] Under the December 21, 2006, Notice of Proposed Rulemaking, the regulations directed railroads to evaluate the safety and security of the surveyed lines and make routing decisions based on the review. As initially introduced, the regulations represented a tightening of the voluntary approach previously codified under HM-232. The express purpose of the regulation was to ensure that railroads select reroutes that have the fewest safety and security risks.[106] In the summary included with the Notice of Proposed Rulemaking, DOT briefly described that the regulations

> require rail carriers to compile annual data on specified shipments of hazardous materials, use the data to analyze safety and security risks along rail transportation routes where those materials are transported, assess alternative routing options, and make routing decisions based on those assessments.[107]

The outlined regulations called for railroads to collect commodity data annually and review all routes on which large quantities of explosives, radioactive materials, and TIH cargoes traveled; additionally, they called for a review of alternate commercially practicable routes.[108] Railroads would then select the route that presents the fewest safety and security risks for hazmat transportation.[109] The proposed regulations provided guidance as to how railroads should conduct route reviews. The language contained in the proposed appendix D to 49 CFR 172 lists 27 different "rail risk analysis factors" to be considered during annual evaluations of current and alternate routes. The list of factors was wide-ranging, including quality of track, traffic density, volume of hazmat material shipped, and known threats and mitigation measures in place.[110] Railroads had to include in writing analysis of these 27 different elements in their annual reviews.[111] Additionally, the proposed regulations provided the FRA with enforcement powers. As part of its routine review and evaluation of rail operations during site visits, the FRA was enabled to review the routing analysis conducted by the railroad and, upon findings of noncompliance, impose alternate routes, enact operational modifications, or levy civil penalties.[112]

Congress Rewrites the Rules

The proposed regulations underwent important modifications between their initial proposal in April 2006 and enactment of the Final Rule in November 2008. During the review and comment period, activists successfully

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

marshaled support for key concessions. Environmental groups, mainly Greenpeace and Friends of the Earth, joined cities and states in pushing for modifications to the proposed regulations.[113] In particular, they pushed for regulations to expand the scope of the required analysis to include possible alternative routes. As initially proposed, railroads only needed to examine a single alternative route as part of their annual review—identified as the "next most commercially practicable route over which it has authority to operate"—for each route carrying specified quantities of hazardous cargo.[114] Greenpeace and Friends of the Earth pushed for an analysis that was not limited to the single most economically attractive alternative but rather included *all* alternative routes, including the use of interchange agreements with other railroads (which would expand possible alternative routes). These modifications, if enacted, would greatly expand the scope of the review that railroads were obligated to undertake. Here, they would have to look beyond the lines that they controlled and consider shifting traffic to other railroads via interchange.[115]

Activists also sought to increase the involvement of local communities in routing decisions and make explicit the importance of high-consequence targets adjacent to rail lines in conducting route analysis. Although the proposed regulations explicitly affirmed preemption, activists sought the inclusion of a mandate requiring railroads to consult with local communities in identifying en route risks.[116] Additionally, though the regulations would not mandate rerouting around cities, activists, as a consolation, sought to add language to the regulations identifying the significance of urban areas in making safety and security determinations.[117]

The environmental movement and a host of cities and states offered these modifications during the open comment period following the Notice of Proposed Rulemaking.[118] More importantly, not taking any chance that DOT would ignore their comments in deference to greater flexibility for the rail industry, this loose coalition also backed new federal legislation that would compel the adoption of these modifications.[119] While under DOT review, the newly Democrat-controlled Congress passed the Implementing Recommendations of the 9/11 Commission Act of 2007 (the 9/11 Commission Act).[120] Title 15, Subtitle D of the act, Surface Transportation Security: Hazardous Material and Pipeline Security, directs DOT to include many of the modifications activists were seeking. The act sought to speed up the slow-moving regulatory process. It directed DOT to publish its final rule within the next nine months.[121] Substantively, the act imposed burdens on how the new regulations would operate. The act required that the eventual final regulations compel railroads to consider multiple routes,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

rather than a single alternative route, and possible interchange agreements in assessing alternative routes.[122] In another nod to activists, the act specified that route analysis take into account and consult with state, local, and tribal governments about significant "high-consequence" targets located near the rail lines on which hazardous cargoes travel.[123] The 9/11 Commission Act ensured that DOT would have to accept the concerns articulated by environmentalists and local communities. Although rerouting legislation had previously been introduced numerous times in Congress with little success, the 9/11 Commission Act represented a triumph for Greenpeace and Friends of the Earth.[124] The act stopped short of mandating rerouting around urban areas, but it made explicit the importance of considering urban areas in routing decisions, expanded the scope of alternate routes that railroads must examine to select the safest and most secure route, and provided a place for local communities in routing decisions.

Qualified Victory and Compromise

In response to the 9/11 Commission Act, DOT substantially revised the final regulations. The new regulations located in 49 CFR 172 and 174 move away from the essentially toothless and lax regulations first introduced as HM-232 and the modest regulations that had been first floated in the Notice of Proposed Rulemaking following the DC litigation. The final regulations were adopted in 2008. They require railroads transporting specified hazardous cargoes—TIH materials, explosives, and radioactive material—to examine alternate practicable routes and interchange agreements during annual security and safety reviews. Rather than calling on railroads to examine a single alternative line and to study only routes fully under their control, the rule expands the scope of review greatly and, in the process, increases the likelihood that alternative routes will be identified and employed. The revised final regulations also carve out a space for local participation and explicitly state that local cities and states must be consulted in making routing decisions. Railroads must provide a single point of contact to integrate the information provided by local communities and provide their estimations of the risks accompanying different rail routes.[125] Finally, 49 CFR 172, appendix D specified that high-consequence targets (read: cities) are to be considered in determining safe and secure routes.[126]

Though railroads fought these changes, the final regulations are not entirely inhospitable to their prerogatives.[127] Under the new terms, mandatory rerouting is not put in place, and preemption is made explicit and unambiguous.[128] In this fashion, new regulations spare railroads from the most aggressive local rerouting efforts. The regulations also preserve

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

a certain amount of autonomy for the railroads in examining alternate routes. The 27 factors identified in 49 CFR 172, appendix D are not organized in any schematic way.[129] Though each factor must be addressed in writing and is subject to FRA review, the regulations do not provide a clear framework for weighing the relative importance of listed factors.

The Politics of Green Security

As in the other case studies, the central question or set of questions to discuss when examining the bureaucratization of risk returns to politics and power: Who defines the new techniques of control employed to domesticate the uncertainty of terrorism? What values are embedded within these new policies and procedures? What types of social relations are enacted through security practices? Ultimately, the introduction of new rail hazmat security regulations represents a qualified, though important, victory for environmental activists and their allies in local and federal government. The debates over hazmat shipments were something of a referendum on rail deregulation—they grappled with both the material consequences of deregulation (the increasing volumes of hazardous materials that moved near or through urban centers) and the larger reordering of power that deregulation enabled (that is, the increasing power of the rail companies to act as they saw fit and the elevation of the market over collective forms of supervision and control).

The final new regulations governing the security of rail cargoes of hazardous materials do not include mandatory rerouting.[130] Yet in important respects, activists are the key authors of these new security regulations. Through dogged work at the local, state, and federal levels, they secured important concessions over the objections and reluctance of industry and DOT. Here, the shift in power that deregulation enacted is somewhat rolled back: Rerouting regulation *is itself* a form of democratization—it puts railroads under public scrutiny and makes them publicly accountable. Now, railroads must contend with and take seriously the concerns of *other* infrastructure publics. Cities, towns, and states have a say in how certain chemicals are routed. Regulations are a counterweight to the market—they are an explicit rejection of the idea that the market and the drive for efficiency alone can and should guide how infrastructures are governed. The final DOT security regulations move significantly away from the loose voluntary approach initially championed by industry, the Bush administration, and the DOT and work to limit the risks associated with the influx of hazardous materials transported by rail. By appropriating the language

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

of national security and building coalitions with politicians at the city and state level, as well as with key Democratic senators, environmentalists were able to write into new security regulations the mandatory consultation with local governments, the annual review of expanded alternate routes and interchange agreements, and the consideration of urban areas in route assessments. These are not trivial changes. Taken together, these provisions offer a significant transformation of the governance of hazardous materials transportation. New regulations impose burdens requiring railroads to conduct annual reviews of routing options and justify the selection of routes based on safety and security, while FRA enforcement creates liability for their noncompliance.

The introduction of a new mandate for DOT to regulate rail security kept alive the possibility for further action at some point in the future. In 2015, this possibility became a reality.[131] A series of destructive and high-profile accidents involving rail shipments of crude oil thrust attention back onto the safety and security of rail shipments of hazardous materials.[132] In 2013, a train carrying 72 cars of crude oil derailed in the town of Lac-Mégantic, Quebec (see figure 5.2).[133] The accident killed 47 people and destroyed 40 buildings, leaving a hole in the middle of the town. A year later, in 2014, a CSX train hauling 104 tank cars filled with crude oil derailed in downtown Lynchburg, Virginia. One car was breached, and 29,868 gal. of oil spilled into the river and caught fire. No one was killed, but the accident led to millions of dollars in environmental damages and cleanup costs.[134] These and other incidents spurred calls for action.[135] Critics, led again by environmental activists, pointed out that the domestic oil boom was leading to an influx of crude oil on the railways.[136] Between 2011 and 2012, the amount of crude oil shipped via rail increased by a stunning 423% (shipments of ethanol, another flammable hazard, likewise spiked).[137] The regulations put in place in 2008 served as a model for regulating shipments of crude oil and ethanol (and other flammable materials). The regulations initially driven by concerns over toxic materials and terrorism were effectively expanded to cover a larger list of compounds, including bulk shipments of flammable gases and flammable liquids.[138] The battles of the early 2000s paid dividends. Since 2015 these controls have expanded to cover a wider swath of hazardous materials.

The threat of terrorism destabilized rail operations and called into question the existing regime of safety regulations and practices that had evolved for nearly a century. It did not do so automatically—it took activists (and their partners) working through local, state, and federal venues

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Figure 5.2
Rail derailment in downtown Lac-Mégantic, Quebec, July 6, 2013. Image courtesy of AP Photo/The Canadian Press, Paul Chiasson.

to press the issue and transform fear into a workable program of reform. The fight over rerouting is about more than the specific minutiae of hazmat policy; rather, it is also about the role of the public in shaping policy and managing infrastructure. Here, activists were able to appropriate the vernacular of security—seize on the salient, though difficult to define, threat of terrorism and anxiety about the insecurity of infrastructure—in order to substantively change transportation policy. The activists were successful: they were able to shift the tenor of regulations in significant and, it appears, lasting ways. In early 2000, Greenpeace activists scaled a fence of a Dow Chemical plant outside of Baton Rouge, Louisiana, to draw attention to the security risks associated with toxic chemicals. Their "raid" drew little attention or substantive change in how chemicals are produced, transported, or used.[139] After 9/11, however, these concerns appeared far more legitimate and reasonable.[140] Security provided activists with a say in policy that they might not have otherwise had.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

6

Regulating Cybersecurity: The Unexpected Remaking of Electric Power

Nothing seems to be updating on the computers. … We've had people calling and reporting trips and nothing seems to be updating in the event summary. … I think we've got something seriously sick.
—FirstEnergy transmission operator to IT department, August 14, 2003[1]

On August 14, 2003, the evening commute for millions of New Yorkers did not go as planned. Subways stopped running, elevators stalled in mid-descent, and traffic congestion made driving nearly impossible. The power was out. Thousands abandoned their typical commute and set out on foot, streaming across the Brooklyn Bridge on their way home. Others decided not to brave the hectic conditions and bunked wherever they could.[2] The largest blackout in the nation's history stretched across eight states and parts of Canada, leaving over 50 million people without power.[3]

The blackout was a classic normal accident. It was set in motion by a mix of mundane and decidedly unspectacular failures: an employee at the Midwest Independent System Operator (MISO) turned off MISO's state estimator, a computer system that monitors system contingencies, in order to troubleshoot an unrelated problem and then forgot to turn it back on. At around this time, Eastlake5, a power generator in northern Ohio, tripped due to operator error. This normally would not have been too significant. FirstEnergy should have been able to import enough power to cover the loss of Eastlake5. But in quick succession, falling trees snapped a number of high-voltage lines.[4] The MISO employee's failure to switch the state estimator back on and unrelated computer failures at FirstEnergy now took on much more significance. They made both the line outages and the failure of Eastlake5 difficult to account for, leading to further problems. The comedy of errors—each unremarkable on its own and largely unrelated—continued to compound. A series of seemingly small and local failures cascaded through the system, throwing transmission lines and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

generators off-line. The risks of a tightly coupled and complex electric power system became stark: these apparently minor failures turned out to be fatal. The deregulation of electric power had replaced the staid utility system with vast networks of tightly integrated players—generators, transmission operators, distribution systems, marketing companies, and others—lashed together through technical and nontechnical linkages. The fragility of this new constellation now came rushing into view. A few tree branches fall, a computer system is accidentally turned off, an operator makes an unfortunate but not entirely unexpected mistake and then, suddenly, the lights go dark and 50 million people across the U.S. and Canada cannot turn them back on.

The outage dwarfed the 1977 New York blackout. It had significant regional—rather than local—impacts. Shortly after 4:00 p.m. on August 14, 2003, New York, Toronto, Cleveland, Detroit, and many other cities came face-to-face with life without electricity as a cascading power failure moved from Ohio to parts of the Northeast, to the Midwest, and to Ontario.[5] Speaking in San Diego, President Bush promised a thorough review of the nation's electrical system.[6]

* * * *

This chapter examines the reorganization of electric power that followed the passage of the Energy Policy Act of 2005. The new law transformed federal regulatory powers governing the nation's electrical system and called for the creation of the first set of mandatory cybersecurity regulations—known as the Critical Infrastructure Protection (CIP) Standards—for the electric power grid. The law was initially driven by—and on paper very much appeared to be indebted to—industry interests. The *Toronto Star* derisively called the new law the "Leave No Energy Company Behind Act" and dubbed it a "porkfest of subsidies" for the energy sector.[7] However, what looked on its face to be an attempt by the electric power industry to further consolidate its power morphed into something much different—new forms of accountability and public oversight of the electric power industry. Regulators from the Federal Energy Regulatory Commission (FERC) took a new set of thin administrative powers and transformed them into a robust system of checks and balances. Industry had drafted the federal legislation to leave regulators with a marginal role. But federal regulators had different ideas. They turned a rubber stamp into a hammer.

The development of the new cybersecurity regulations for the electric power grid reveals an important story about the possibilities of security

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

politics. The transformation of infrastructures into dangerous things made the 2003 U.S.-Canada blackout legible in a new way. The entwined cultural, institutional, and organizational changes that unspooled after 9/11 made it possible to view the power grid as a target of malicious subversion. The blackout became not an aberration or freak accident but something closer to a warning: a sign of the fragility of the grid—a sign of what *might* happen if enterprising terrorists or other malicious actors set their minds to attacking the power system. This framing was vital to the Energy Policy Act of 2005. It was used to justify layering new forms of security protections and a new system of regulatory power onto the power system. These changes created a space and an opportunity for federal regulators to seize an important oversight role. Ultimately, FERC leveraged its limited powers to implement cybersecurity regulations that were significantly tighter than the standards proposed by the industry. FERC bucked industry preference for limited administrative regulations containing ample loopholes and instead secured comprehensive cybersecurity controls. These new regulations directly confronted the social and technical challenges unleashed by deregulation (see chapters 1 and 2). Now, the unintended consequences of decades of technological and institutional change were called to account. New robust cybersecurity regulations created an avenue for ongoing public review and participation in the oversight of electric power. Like the case of freight rail (see chapter 5), concerns over terrorism led to the creation of new forms of accountability that unexpectedly shuffled and reordered the power between industry and other publics. To the surprise of industry insiders and many skeptics, security concerns were leveraged to reinvigorate public oversight of the industry. These changes were, as we will see, anything but a foregone conclusion.

Reforming Electric Power: The Electric Power Industry Makes Its Case—and Gets Nowhere

By the late 1990s, electric power had entered a brave new world. Deregulation had radically altered the industry. Vertical monopolies were replaced by new centrally managed regional markets. This shake-up (detailed in chapter 2) unfolded over decades, but by the end of the 1990s, industry incumbents were getting nervous. This new setup seemed to teeter on the edge of failure. Where before electric power had been defined by a fairly limited club of traditional utilities supervising and controlling their own systems, now thousands of new and different organizations worked to keep the lights on. This transition gave industry players pause. So much

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

has to go *right* for electric power to work, and this new, complex ecosystem appeared to be ripe (and indeed was) for accidents or unscrupulous manipulation and gaming of the deregulated system for profit. The Enron scandal and the 2003 blackout would prove these were anything but idle fears.

In the late 1990s, key industry players drafted model federal legislation to help manage some of the unintended consequences of this competitive new world.[8] The North American Electric Reliability Council (NERC) oversaw the development of the proposed legislation in what came to be called the *NERC consensus language*. NERC had long worked as a voluntary industry association and forum for power companies. It had been created by the electric power industry after the 1965 Northeast blackout to promote industry best practices and oversee the development of voluntary standards.[9] In the late 1990s, NERC worked with all corners of the industry—including the Edison Electric Institute (the industry trade association that represents private electric companies), the American Public Power Association (which represents publicly owned utilities), the Electric Consumers Resource Council (a trade association representing large industrial power customers), and state and federal regulators—to develop model legislation.[10] The need for reform was clear. As T. J. Glauthier, deputy secretary of Energy, Department of Energy, noted in testimony before Congress in 1999: "As we move to a more competitive environment, the reliability of our bulk power systems can no longer be entrusted to voluntary standards."[11] This changing landscape made some sort of mandatory reliability rules necessary. As backers of the NERC proposal repeatedly noted in congressional testimony, electric power had become too complex and too reliant on thousands of different interdependent players with different agendas and interests to be left to voluntary standards alone.

The centerpiece of the NERC proposal was self-regulation. The electric power industry would police itself. The model legislation sought to impose binding rules on these new players in order to make sure there were no "weak links" that could undermine or jeopardize the reliability of the larger interconnected power system. The proposed model legislation would transform NERC. Under the plan, it would be designated as an electric reliability organization (ERO). NERC would then be able to legally enforce the standards developed by industry. In effect, NERC would keep doing what it had been doing for years—serving as a venue for industry to hash out its own rules—only now the standards it developed would be legally binding. The industry trade association would now have real teeth. Under the proposed terms, NERC would oversee a process in which industry members would draft, propose, and vote on

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

possible mandatory and legally binding reliability standards. NERC, and not federal regulators, would then enforce these standards.[12]

This was a deeply conservative response to the challenges unleashed by deregulation. Federal regulators—FERC—would have little power and little say in shaping reliability regulations. They would review the standards that NERC eventually submitted against very narrow criteria, making sure they were developed according to the guidelines that the industry put in place and, at most, looking for procedural missteps. But the draft text was explicit: federal regulators would defer to industry on the *substance* of regulations. Regulators would wield a rubber stamp. Their approval would transform the standards that industry developed into legally binding rules, but FERC would have little opportunity to actively shape the content of standards. Deregulation had sloughed off many of the regulations and controls that had long governed electric power. Industry was not about to advocate for tighter federal regulations now. If anything, the NERC consensus language would give industry *even more power* to control and shape electric power as they saw fit, with little meaningful public oversight or accountability.

Industry heavyweights, state public utility commissioners, and federal regulators all lined up in support for the NERC consensus language.[13] During the 2000 election, candidate George W. Bush made energy reform a key priority.[14] After the election, President Bush quickly created the National Energy Policy Development Group (NEPDG), chaired by Vice President Dick Cheney, and put together a comprehensive plan for reform.[15] The group included cabinet-level participants and a cadre of industry representatives and lobbyists.[16] The deliberations of the group were secret and controversial. The industry representatives and lobbyists were not technically members of the NEPDG, a formal designation designed to prevent public disclosure of their participation.[17] A years-long legal battle over public disclosure of the NEPDG's records and the scope of executive privilege culminated in a ruling in favor of the vice president and the nondisclosure of the NEPDG documents.[18] Nonetheless, information about the group trickled out. The picture that emerged showed industry and government working hand in glove. The NEPDG met extensively with titans of the energy industry. Exxon Mobile, Enron, Duke Energy, Florida Power & Light, the American Petroleum Institute, the Interstate Natural Gas Association of America, and others representing the power industry had significant input into the group's deliberations.[19] Environmental groups were, on the contrary, given a cursory meeting (Vice President Cheney did not attend, and half of the allotted meeting time was taken up by

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

introductions).[20] The NEPDG produced a sweeping report titled the *National Energy Policy*. It substantially reflected the priorities of industry, including recommending opening the Arctic National Wildlife Refuge to drilling, offering subsidies for coal, and ramping up support for oil and gas production.[21] Unsurprisingly, the report also supported the adoption of the NERC consensus language that industry had been flogging for a number of years. In its litany of recommendations, the report called for legislation based on the principles outlined in the draft legislation.[22]

Despite the powerful backing of the executive branch, industry, and federal and state regulators, the NERC consensus language stalled. It was added to bill after bill in Congress. But the language could not get passed. Over and over again, the NERC consensus language died in committee. By as early as 1999, FERC chairman James Hoecker was starting to sound weary, remarking in congressional testimony that he had been pushing this same proposal before both the House of Representatives and the Senate for the better part of two years.[23] By 2003 the model language was starting to look like it might be a dead end … and then the blackout happened.

The August 2003 Blackout: Revisiting Electric Power

The 2003 blackout was the worst power outage in the nation's history. Over 50 million people in the U.S. and Canada lost power, and 508 generators at 265 plants fell off-line, affecting 61,800 MW of electric load.[24] The blackout's economic impact was staggering; estimates place losses at between $4 and $10 billion dollars.[25] On August 15, the day after the blackout, President Bush and Canadian prime minister Jean Chrétien announced the formation of the U.S.-Canada Power System Outage Task Force. The task force was charged with investigating the causes of the blackout and offering recommendations on how to improve the reliability of the electric power system.[26] As part of its work, it would investigate the blackout and conduct a broad review of the electric power system.[27] U.S. Secretary of Energy Spencer Abraham and Herb Dhaliwal, the Canadian minister of natural resources, were appointed to lead the task force.

The task force divided its work across three working groups: the Electric System Working Group, Nuclear Working Group, and Security Working Group.[28] Public-sector experts drawn from the Department of Energy, Nuclear Regulatory Commission, FERC, Federal Bureau of Investigation, Department of Homeland Security, U.S. national labs, state utility boards, and their Canadian counterparts staffed the working groups and worked in close collaboration with industry.[29]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The task force released its interim report in November 2003 and its final report in April 2004.[30] The final report identified a mix of technical failures, human errors, and institutional factors as contributing causes.[31] The task force found both low- and high-tech failures. It placed the blame on both faulty vegetation practices—tree trimming—and various computer glitches and errors.[32] The failure was not merely technical: at critical moments, human error—failure to turn critical equipment back on, failure of an IT team to recognize that their system reboot had failed to fix a stalled alarm, and other decisions or moments of inaction contributed to the outage.[33] The failings ran deep. The task force found pervasive institutional challenges. It echoed a by-now-familiar complaint: the lax and ambiguous regime of voluntary regulations that oversaw electric power was ill-suited to confront the challenges of ensuring that a competitive electric power system remained reliable. In examining the practices of FirstEnergy, the MISO, and PJM Interconnection—all key players in the outage—the task force found multiple violations of the industry's voluntary reliability standards. In other cases, the standards on the books were so ambiguous that they made meaningful compliance difficult.[34]

Terrorism, Cybersecurity, and the U.S.-Canada Power System Outage Task Force

The task force examined another possible source behind the massive outage: terrorism. The post-9/11 cultural and institutional recalibration toward questions of homeland security and fears over terrorism hung over the task force's work. The threat of terrorism now provided a powerful backdrop for nearly *all* discussions of infrastructure policy. After 9/11, major infrastructure failures were greeted with foreboding: Could this be another terrorist attack?[35] The power outage initially sparked such fears. On the day of the blackout, the New York Police Department activated its terrorism-response plans and deployed armed teams to protect high-profile targets, such as the New York Stock Exchange.[36] It was a tense moment. Only a few weeks earlier in July, U.S. and Canadian government officials had issued warnings to the energy sector based on collected intelligence indicating that Al-Qaeda might attack power plants.[37] However, in remarks delivered in San Diego several hours after the blackout, President Bush attempted to quell fears of terrorism in a brief statement to reporters, noting: "One thing I think I can say for certain is that this was not a terrorist act."[38] Yet concerns lingered. On August 18, *Al-Hayat*, an Egyptian news outlet, reprinted a communiqué attributed to Al-Qaeda claiming credit for the power outage.[39] Similar claims appeared in various news outlets in the following weeks and months.[40]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The possibility that the blackout *could* have been caused by a terrorist act informed the task force's work and ultimately shaped its recommendations. The task force examined seriously charges that the outage could have been caused by terrorism. In creating the task force, President Bush and Prime Minister Chrétien appointed three U.S. and three Canadian public officials to serve directly under the leadership of Secretary Abraham and Minister Dhaliwal. Among the high-profile U.S. appointees was Secretary Tom Ridge of the Department of Homeland Security. The selection of Secretary Ridge highlighted the prioritization of security and terrorism within the task force.[41] Similarly, the creation and designation of the Security Working Group signaled the prominence that security concerns would hold within the inquiry—and it underlined the broader prominence that security now held for discussions of infrastructure.[42] The Security Working Group ultimately confirmed President Bush's initial assertion that terrorism played no role in the outage. The Working Group found no evidence supporting published claims of responsibility and discounted any role of malicious activity.[43] But, despite concluding that this was not a terrorist attack, the task force nonetheless placed security concerns front and center in its eventual report and recommendations.

The task force moved beyond the particulars of the 2003 blackout to offer a more general assessment of the power system. The unbound imagination that now characterized much post-9/11 thinking was on full display: rather than narrowing its exploration to what had happened, the task force started to consider what was simply possible. It found reasons to worry. The task force found no concrete evidence of foul play, but it did find significant opportunities for real harm. Hacking the computer systems crucial to the electric power system could result in great damage. The task force, in an analysis that would have been familiar to staffers working nearly a decade earlier on the President's Commission on Critical Infrastructure Protection (see chapter 3), saw that the use of information and communication technologies (ICTs) created openings for enterprising terrorists to manipulate the power grid. The Security Working Group seized on the presence of such vulnerabilities as a significant area needing improvement.[44] The final report noted that "the increased reliance on IT by critical infrastructure sectors, including the energy sector, has increased the vulnerability of these systems to disruption via cyber means."[45] It noted that supervisory control and data acquisition (SCADA) systems are particularly susceptible to corruption. For the task force, the transformation of ICTs within electric power from standalone proprietary systems to generative, multipurpose machines operating

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

across corporate networks and the Internet created new cybersecurity challenges.[46] This new technological ecosystem, in the task force's view, could be exploited to undermine the functionality of the grid. The report readily accepted that electric power was a target, noting: "The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting this system."[47] In addition to targeted attacks, the spread of malware designed to exploit flaws in common operating systems and software applications could incidentally threaten electric power systems, despite not specifically being tailored for this sort of purpose.[48] The task force, both implicitly and explicitly, wrestled with the challenges presented by the reorganization of electric power. It grappled with a difficult question: Given the broader structural changes in the industry and the ongoing merger of operational technology (OT) with a more conventional information technology (IT) environment, how could electric power be secured?

The task force's discussion of cybersecurity was important. It reworked traditional notions of what security means within the electric power sector.[49] Historically, *security* had a fairly clear meaning in the context of electric power. It was defined as "the ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements."[50] Security, in this sense, was taken to relate to system stability and reliability. A secure system within this framework meant planning for and having on hand adequate resources, particularly generating capacity, to meet fluctuating demand. Security practices comprised the difficult work of keeping the system in a state of balance that matched generation and consumption. System security confronted a range of possible disruptions, including operator error, spikes in demand, poor weather, and accidents—but it did not focus primarily on intentional disruptions. Under this rubric, a secure system is one that has adequate capacity to meet demand.

In a different vein, the NEPDG—Vice President Cheney's energy advisory group—had made energy security a key focus of its report back in May 2001. In that document, *energy security* was taken to mean securing access to cheap and reliable sources of power. As a practical matter, the NEPDG used energy security to argue for a reduction in oil imports in favor of increasing domestic production, exploring untapped and underdeveloped oil reserves across the globe, and strengthening trade with oil-producing nations.[51] That document had a few boilerplate sentences about infrastructure security and the perils of intentional disruption.[52] But the bulk of the discussion of energy security in this earlier report was

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

tethered to ideas about market volatility and resource scarcity. Energy *insecurity*, in this telling, was about spikes in prices for oil and possible production shortfalls. Energy security, as of May 2001, was a question of ramping up domestic production and opening up untapped resources.

The task force transformed the meaning of *security* within discussions of electric power: it split from both the more familiar use of security within electric power operations and the recently put forward notion of energy security found in Vice President Cheney's NEPDG report. The U.S.-Canada Power System Outage Task Force adopted a different notion of security. It aligned security with malicious activity, contemporary fears about terrorism, and attacks targeting infrastructure. In a conceptual remapping, it employed in its report what had become a more colloquial notion of security that means something closer to "defense against intentional attack." This was quietly revolutionary. Here, the idea of a "secure" system became something quite different: rather than emphasizing resource adequacy, security now became linked with authorized access, defensive postures designed to repel or discourage saboteurs, and the broader interests of geostrategic security. This was an important shift. By explicitly and implicitly emphasizing the threat of terrorism and malicious intentional disruption, the task force expanded the meaning of security to include a larger set of contingences that blurred conversations about electric power reliability with the larger ongoing discussion about terrorism and infrastructure security. Now, the task force argued, security planning must confront the possibility of enterprising intentional disruption. For decades, operators worried about the impact of storms, demand fluctuations, and accidents on the electric power system; now, they began to worry about terrorism.

The conceptual transformation mapped out in the blackout report was radical. It led the task force to question the standard approach to contingency management that the industry had long used, and it led to an intense focus on questions about cybersecurity. Historically, power operators relied on what is known as the *N-1 Criterion* to guide reliable operation. Long used by operators and written into the industry's voluntary guidelines as NERC "Operating Policy 2.A—Transmission Operations," N-1 directs operators to ensure that at any moment their system can withstand the loss of the *single* most critical transmission or generation asset without significant disruption of service.[53] N-1, or normal operating conditions minus one, provides a margin of error: it is intended to ensure that systems can absorb the single worst outage or contingency at any given moment without lapsing into a large-scale cascading failure.[54] This rubric became encoded

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

within standard operating procedures across the industry. During day-to-day operation, controllers continually reevaluate and adjust system performance as system conditions change (demand shifts, assets come online or move off-line, and so on) in order to ensure that adequate resources are always available. As conditions shift, operators continually adapt to a new N-1 state—that is, they make adjustments to survive the current single largest contingency within the reconfigured system conditions. Ideally, these changes are supposed to occur within 30 minutes, giving operators a short window to accommodate changing conditions on the ground and make sure their system is robust.[55]

The task force's redefinition of security chipped away at the utility of N-1. This approach to contingency management works well to confront random failures. N-1 as a planning guide assumes that when the mundane failures that have traditionally occupied the worries of operators occur—high winds, storms, operator error, and the like—they will only trip a single asset at a time.[56] Malicious attacks, however, do not always follow a random distribution. Storms do not coordinate and plan; terrorists might. Targeted assaults can occur at multiple locations and hit many assets simultaneously to maximize harm. In confronting terrorism, multiple simultaneous contingences, rather than just the single worst contingency, start to appear as legitimate possibilities.[57] What's worse, as NERC's chief security officer would soon note, the diffusion of common ICTs across the industry created possibilities for horizontal disruptions that could ripple across and within connected systems.[58] Malware might target and manipulate not just a single controller within a single utility; it could potentially target *all* of the power companies that use a similar hardware and software mix. Rather than disabling or disrupting a single isolated system, this could cause failures at multiple points within the larger electric power system at the same time. These types of failures are not well accounted for under N-1.[59] The task force argued that terrorism and the new ICT landscape created different challenges. The possibility of targeted simultaneous attack or horizontal failures of standard computer equipment go beyond the scope of N-1.

The task force followed the by-now-familiar testimony of industry insiders and regulators and concluded that an overhaul of the governance of electric power was long overdue. The traditional approaches to managing system reliability no longer seemed to fit. This was not a new insight. But the task force did offer a new pressing rationale for mandatory standards: security. Voluntary standards and N-1 might have made sense once upon a time, but as the task force concluded, fears over

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

terrorism—wherein malicious actors are assumed to always be lying in wait—combined with a technological system rife with exploitable vulnerabilities seemed to call for a drastically new approach. If the industry's standard way of managing contingencies was no longer useful, what might take its place? The task force had a suggestion: mandatory standards and new specific cybersecurity regulations.

Mandatory Regulations and Cybersecurity: The Task Force's Recommendations

The U.S.-Canada Power System Outage Task Force's final report provided a path for reform. It offered fundamental recommendations for overhauling the governance of electric power and presented specific recommendations for confronting the particular challenges of cybersecurity. The final report contained 46 recommendations.[60] At the highest level, the recommendations called for an overhaul of the process of developing and enforcing reliability standards. Voluntary measures and reliability standards had governed electric power for decades.[61] The task force recommended scrapping this approach. It noted that voluntary standards were routinely ignored with little punishment. NERC—the industry trade group—developed these standards, but they did not carry the force of law, and NERC had few tools to meaningfully address noncompliance.[62] The task force turned and endorsed the model legislation developed (to no avail) years before and recommended that NERC be given new legally binding power to develop and enforce reliability standards for the industry.

It was unsurprising to see the blackout task force yet again dust off the NERC consensus language. This language had become de rigueur for nearly *all* proposals to overhaul electric power. The task force's recommendations closely followed the NERC consensus language. In keeping with what by now had become a standard set of recommendations, the task force called for a staggered regulatory structure: NERC would internally create and enforce mandatory reliability standards in consultation with industry, and federal regulators, FERC, would have limited power to accept or reject the NERC-developed standards.[63] Under the task force's model, federal regulators would certify a single entity as the Electric Reliability Organization (ERO). The ERO would represent the industry and develop and enforce mandatory reliability regulations. The task force made plain in its final report that the ERO concept was designed and proposed with the understanding that NERC would fill this role.[64] The power industry would self-police. The industry would work through the ERO to develop reliability standards and enforce compliance. The role for

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

federal regulators was narrowly drawn: FERC would have the authority to accept or deny proposed reliability standards but not draft or develop regulations; it would be called to defer to industry in defining the content of the standards.[65] Within this scheme, FERC's approval would give industry-developed regulations legal standing. The proposed scheme would enhance—and not diminish—the power of industry: it would govern itself.

The task force did, however, move beyond the developed model legislation. Thirteen of the 46 recommendations in the report specifically addressed a new topic: cybersecurity.[66] Just as it had with the more general recommendations, the task force once again followed industry's lead. NERC had already been working on some modest voluntary cybersecurity guidelines before the blackout. In a coincidence, on August 13, 2003, *the day before the blackout*, NERC released its first voluntary cybersecurity standards, Urgent Action Standard 1200 (UA 1200).[67] UA 1200 contained 16 different sections concerning access controls, critical asset identification, and training. It was nonspecific. It asked relevant players to create and document plans, but it said little about what those plans should actually look like. Having a plan on file was enough.[68] The task force did not provide a review of UA 1200, but it nonetheless advocated adopting the mandatory reliability standards as a first step in addressing the cybersecurity issues now plaguing the industry.[69]

The NERC consensus language was not dead after all—post-9/11 fears and the work of the blackout task force gave it a new urgency, a new rationale, and a new life.

The Energy Policy Act of 2005: Reforms—Intended and Otherwise

On August 8, 2005, President George W. Bush signed the Energy Policy Act of 2005 into law. It was a significant piece of legislation.[70] In over 1,700 pages of text, it promised substantial changes to U.S. energy policy. In many ways the law appeared to be the apotheosis of deregulatory zeal. It continued the now long-standing trend of removing or relaxing administrative controls over electric power and serving up generous benefits to powerful industry players. The law offered over $14 billion in tax breaks for the oil, gas, and coal industries (it provided little support for renewable energy).[71] It loosened or cut environmental protections and created exemptions to clean water laws for the oil and gas industries.[72] The new law repealed the Public Utilities Holding Company Act of 1935—the key Depression-era law that had limited consolidation within electric power (see chapter 1). The new law was largely shaped by—and in some cases

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

directly drafted by—the energy industry. The report originally produced by Vice President Cheney's NEPDG provided a rough blueprint for the new legislation. The law contained most—but not all—of the recommendations included in that report.[73] The revolving door of energy executives who had worked with Vice President Cheney's group—including representatives from Constellation Energy Group, British Petroleum, and many others—to draft the *National Energy Policy* report could not have been happier.[74] Four years after the fact, their vision had been written into law.

Critics saw a disaster. Just as they had criticized the Cheney report years earlier, they attacked the law. Anna Aurilio, legislative director for the Public Interest Research Group, a consumer-focused nonprofit formed by Ralph Nader in the 1970s, tartly noted that "it's Christmas in August for big energy, and consumers get lumps of coal."[75] Environmental groups were equally furious.

But the new law had not only been shaped by wheeling-and-dealing industry executives. The 2003 blackout and the larger post-9/11 recasting of infrastructures as dangerous things played an important role. At a ceremony at the Department of Energy's Sandia National Laboratories in Albuquerque, New Mexico, President Bush touted the economic impact of the bill. Bush noted that the bill would help lower energy costs and support a growing economy. But the rhetoric of security was not lost in the mix. Bush was clear, stating: "It's an economic bill, but … it's also a national security bill."[76]

The NERC consensus language *finally* became law. Title XII of the act, known as the Electricity Modernization Act of 2005, for the first time granted authority to the industry to create and enforce their own legally binding mandatory reliability standards.[77] For nearly a decade, the industry had been trying to get some version of this legislation passed. The task force's work and the new post-9/11 context were crucial. It freighted the proposal with a new pressing rationale: protection against terrorism. As in the case of freight rail and the postal system, security concerns amplified and legitimized ideas that had already been circulating.

The Energy Policy Act amended Section 215 of the Federal Power Act. The law called for the development of mandatory reliability standards for the bulk power system and, in particular, required new cybersecurity standards.[78] It specified that reliability standards cover all the facilities and control systems necessary for the reliable operation of the bulk power system or portions of the bulk power system. Under the terms of the new law, generation and transmission were included within the "bulk power system," while distribution to end users was not covered. The text of the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

law made it clear that reliability standards should be designed to support the operation of the interconnected power system such that sudden disturbances will not lead to cascading failure.[79]

The Energy Policy Act followed the template set by NERC and its industry partners (and the U.S.-Canada Power System Outage Task Force): FERC is given limited powers; industry controls—or is supposed to control—the drafting and enforcement of reliability standards. The act called for FERC to certify the ERO. Any entity could apply to become the ERO, but it was clear that NERC was going to be the ERO.[80] Once certified, the ERO can file reliability standards with FERC for approval. In examining the standard, FERC can approve the standard if it finds that it is just, reasonable, and in the public interest or remand the standard back to the ERO for further consideration. FERC's power is limited: it cannot draft reliability standards but rather only approve or remand. Additionally, FERC's review criteria are narrow. FERC is bound to give "due weight to the technical expertise" of the ERO when examining a proposed standard.[81] FERC is specifically instructed to defer on technical matters of content to the ERO. FERC can, however, upon its own initiative or in response to a received complaint, direct the ERO to develop a reliability standard.[82] But again, regulators cannot dictate the content or terms of the standard: they must defer to the technical competence of the ERO. The act also specified that the ERO is responsible for enforcement and can levy penalties on any covered entity found to be in noncompliance, subject to FERC review.[83]

The Energy Policy Act explicitly embraced cybersecurity within its purview. This was a new wrinkle not found in the earlier model legislation. The new law required the ERO to develop reliability standards that apply to intentional cyberattacks or what it termed a "cybersecurity incident."[84] It fully adopted the reworked notion of security discussed by the blackout task force. It defined a cybersecurity incident as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of these programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk-power system."[85] Though the act generally left the content of reliability standards to be determined, it singled out cybersecurity as an area where the ERO *must* develop standards.

The legislation sought to preserve the power of the industry. The Energy Policy Act supported a well-worn path: giving the electric power industry more power. Similar to the discussion of hazardous materials transportation in chapter 5, the threat of terrorism was used to justify an expansion of regulatory powers into a new domain: security. Unlike the expansion of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the Department of Transportation's power, which included a broad security mandate, the Energy Policy Act of 2005 took pains to limit the role of federal regulators in devising new security regulations. The law created a regulatory structure that supported the centrality of industry in the regulatory process. This was firmly in line with the broader promarket restructuring that occurred as part of deregulation. Federal regulators, it seemed, would have little to do but approve whatever NERC passed along. The NERC consensus language, the NEPDG's report, the blackout report, and the Energy Policy Act were each industry-friendly initiatives that sought to increase the power of industry over the terms of the bulk electric power system.

Yet, surprisingly, federal regulators did not sit idly by and rubber-stamp industry-approved reliability standards. On the contrary, in the coming years they leveraged their limited power to substantially redefine the terms of cybersecurity regulations. In doing so, they created greater public involvement and accountability over the operation of the electric power industry and successfully challenged the postderegulation status quo.

Implementing the Energy Policy Act: Regulatory Activism and Transformation

NERC quickly sought recognition as an ERO under the new terms of the Energy Policy Act and moved to convert its existing voluntary guidelines into mandatory reliability standards.[86] But it soon became apparent that the marriage between NERC and FERC was going to be a good deal more contentious than expected. Through the initial approval process, NERC and FERC clashed over the degree of industry autonomy, the specificity of new regulations, and the penalties that would be associated with noncompliance. This was the first test of the freshly minted regulatory process. Both industry and federal regulators attempted to set the tenor and contours of the new relationship.

FERC quickly moved to secure its turf. FERC Order 672, issued February 3, 2006, implemented key portions of the Energy Policy Act by defining the criteria for the certification of an ERO and outlining procedures for the establishment, approval, and enforcement of reliability standards.[87] In the order, FERC asserted a prominent role in defining reliability standards and rejected calls to defer to industry. FERC interpreted the Energy Policy Act broadly. It saw a role for itself that went well beyond simply affirming industry reliability standards. FERC's interpretation cut against the intent behind the long-in-the-works NERC consensus language, the task force recommendations, and, to a large degree, the apparent purpose of the Energy Policy Act. The interpretation was plausible within the boundaries

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

set forth by the act, but it was a generous interpretation. Most importantly, in defining the meaning of *due weight*, the importance of flexibility within mandatory standards, and the scope of remand authority, FERC's order consistently interpreted the Energy Policy Act in ways that favored an enlarged federal role and limited the autonomy and power of industry. This was *not* what industry had been fighting for. For nearly a decade, they had been trying to pass legislation that would allow them to enforce their own rules on their own terms. On paper, it looked like they had gotten everything they wanted. But FERC seemed to have other ideas.

FERC's order reiterated the basic criteria that the Energy Policy Act had set out for the ERO. Order 672 specifies that for an applicant to be certified as the ERO it must be independent, impartial, and open to all industry stakeholders.[88] Under the outlined terms, the ERO will develop reliability standards through open, deliberative processes involving industry stakeholders and then submit them for approval by FERC.[89] But FERC used Order 672 to make clear that the review process was a serious matter that could potentially shape the direction and content of standards. It would not be a rubber stamp. FERC cautioned that it would closely review proposed standards to ensure they did not amount to bland "lowest common denominator" rules that appeased all corners of industry.[90] The Energy Policy Act charges FERC to review proposed reliability standards while giving due weight to the technical expertise of the ERO. There is a tension between the call for FERC to defer to the expertise and the prerogatives of industry, on the one hand, and FERC's duty to perform oversight, on the other. In Order 672, FERC made clear how it intended to resolve these competing values. *Due weight* would not translate into a carte blanche grant of authority to the ERO. Industry hoped that FERC would adopt a limited frame of review and only scrutinize standards for procedural violations related to the development process (i.e., instances when the ERO deviates from its own guidelines). FERC rejected these calls. FERC refused to accept the claim that due weight establishes what is known as a *rebuttable presumption*—that is, a presumption that a finding by the ERO is to be taken as true unless a specific objection against it is offered—in favor of all ERO proposals. Such a position would have tied FERC's hands and allowed it to intervene only when a specific complaint was lodged. FERC rejected the contention that a standard that passes through the internal ERO development and vetting process automatically passes muster as just, reasonable, and nondiscriminatory.[91] Members of industry had wanted just such a presumption. Accepting it would have effectively shut FERC out of *all* substantive decisions, with little to do but certify that

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

industry standards were drafted according to the procedures laid out by industry.[92] FERC refused to be boxed in. Instead, Order 672 staked a strong claim in favor of expanded federal regulatory authority.

FERC's initial order regarding the ERO was a sobering response to the power industry and NERC. It rejected the notion that reliability standards should simply offer general guidelines (as UA 1200 and other voluntary standards had), as opposed to detailed requirements. Industry hoped that FERC would only review the ultimate aims of a proposed standard, rather than conduct an analysis of the precise mechanisms through which such aims are supported. FERC rejected this notion. In some cases, it noted, FERC would have to weigh in on the particularities of standards—not just the end goals.[93] FERC asserted that to ensure that reliability standards are technically sound, uniform, and unambiguous, an examination of implementation would in some cases be indispensable.[94] While FERC accepted the general contention that reliability standards would, in some instances, admit flexibility, it did not accept that this need rendered scrutiny or review of specific operations as beyond the scope of its duties.[95] FERC, here and throughout Order 672, signaled that regulations would in some cases define larger aims *and* in other cases define specific mandates—FERC review could and would take both under examination.[96] Here again, FERC enlarged the scope of its authority to conduct review: it could and would involve itself in substantive issues involving the implementation of reliability standards.

Finally, in Order 672 FERC asserted that the terms of the Energy Policy Act allowed it to not only remand proposed standards but to also include as part of this action a deadline for the ERO to address FERC's concerns and submit a revised standard. This, in time, would prove to be a very useful tool. Though FERC could not directly draft reliability standards, by asserting the right to remand with a deadline for revision and resubmission (and assess penalties if its directions were not followed), FERC carved out a proactive role for itself in the drafting process.[97] By remanding a proposal with a detailed explanation, FERC's hand could now weigh heavily on how industry would develop new standards. Through this process, FERC could become a de facto author of new standards.

Taken together, Order 672 was and is bracing: It offered a broad interpretation of the powers afforded to FERC under the Energy Policy Act, and it significantly qualified industry autonomy. It upset the postderegulation status quo. The Energy Policy Act and the recommendations of the task force intended to ensure that industry would have a decisive say over mandatory reliability standards while setting aside a minor role for

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

federal regulators to approve such standards in order to make enforcement legally binding. Yet in implementing the act, FERC expanded its role. Rather than being content to sit on the sidelines and offer rote approval of standards developed by industry, FERC interjected itself into the substantive work of defining new standards. FERC at each turn consistently offered readings of its authority that supported a greater federal role at the expense of industry and the ERO. Order 672 signaled to industry that the development of mandatory regulations—all regulations, not just cybersecurity regulations—would not be a pro forma exercise. Indeed, as would soon become clear, FERC intended to leave its mark on reliability standards.

Critical Infrastructure Protection Reliability Standards: Security, Autonomy, and the Challenges of Tightly Coupled Complex Systems

The scope and importance of FERC's power grab quickly became clear. Shortly after filing for certification as an ERO, NERC submitted its first batch of proposed mandatory cybersecurity standards, known as the Critical Infrastructure Protection (CIP) Reliability Standards, for FERC review.[98] The proposed CIP standards had already been approved by NERC through industry ballot.[99] This was a key test of FERC's power. Regulators made it clear that the proposed standards were deeply flawed. Subsequent iterations of the standards (version 2.0 and beyond) would have to look far different.[100] FERC had three key complaints. First, it took aim at two particular clauses within the standards—the "reasonable business judgment" clause and the provision that allowed regulated parties to "accept risk," in lieu of mitigating an identified risk, and opt out of the standards. Second, the regulators challenged the vagueness of the standards. Third, they criticized the weak penalties associated with the standards.[101] FERC used its power to push for successive versions of the mandatory reliability standards to be more comprehensive and binding.[102] On each issue, FERC pushed against industry preference. Underlying FERC's arguments on each of the above three issues was the recognition of the unique challenges of ensuring security within complex and tightly coupled networks. For FERC, security concerns were not merely rhetorical gloss: the regulators took concerns about malicious attacks seriously.

NERC's first set of proposed mandatory CIP reliability standards (CIP version 1) created a framework for the identification and protection of critical cyber assets to support the reliable operation of the bulk electric system.[103] In its initial filing, NERC outlined the intended scope of CIP reliability standards by defining the key terms *cyber assets*, *critical*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

assets, and *critical cyber assets*. It defined cyber assets as "programmable electronic devices and communication networks including hardware, software, and data."[104] Critical assets were defined as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."[105] Critical cyber assets were described as "Cyber Assets essential to the reliable operation of Critical Assets.[106] Each standard would apply to the entities playing a role in the generation and transmission of electric power."[107] As drafted, CIP reliability standards were designed to prevent and respond to the malicious disruption or the attempted disruption of critical cyber assets.[108] Version 1 of the CIP standards offered a mix of general and specific requirements. In FERC's summary, the standards "require, among other things, that the responsible entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions."[109] The CIP standards required responsible entities to produce security plans, access control policies, and incident response and recovery plans. More specifically, regulations also called for the use of antimalware software for all critical cyber assets (what it referred to as "Malicious Software Prevention"), the creation of a secure electronic perimeter around all critical cyber assets, and electronic and physical access controls (for an overview of each reliability standard, see table 6.1).[110]

FERC noted that the standards were much improved from the voluntary standards that had previously been in effect. The voluntary standard, UA 1200, covered much of the same ground but relied on self-certification—essentially requiring covered entities to be responsible for determining whether or not they were in compliance—and explicitly disallowed any economic penalties for noncompliance.[111] The proposed mandatory reliability standards moved away somewhat from these limitations, but FERC raised important and significant objections.

Rewriting the Standards: Reasonable Business Judgment and Acceptance of Risk

FERC took issue with language inserted into the proposed standards that provided industry with ample opportunity to, in effect, opt out of meaningful regulation. Each proposed standard contained text indicating that regulated entities may use "reasonable business judgment" in applying the standard.[112] To federal regulators, this was an enormous loophole. NERC outlined the meaning of *reasonable business judgment*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Table 6.1
Proposed cybersecurity standards: CIP-002–CIP-009.

Reliability standard	Title	Purpose	Key requirements
CIP-002–1	Critical Cyber Asset Identification	Identification and documentation of the critical cyber assets associated with the reliable operation of the bulk electric system.	1) Identification of critical cyber assets through "risk-based" methodology. 2) Documentation of critical cyber assets. 3) Annual review.
CIP-003–1	Security Management Control	Development and implementation of minimum security management controls to protect critical cyber assets.	1) Implement and annually review security plan covering standards CIP-002—CIP-009. 2) Implement and document security plan covering access and protection of information relating to critical cyber assets. 3) Implement and document plan for altering critical cyber assets.
CIP-004–1	Personnel and Training	Provide training and risk assessment for all personnel having access to critical cyber assets.	1) All employees, including contractors, with access must receive training. 2.) All personnel with access must receive a risk assessment (background examination). 3) Maintenance of list of personnel with access.
CIP-005–1	Electronic Security Perimeter(s)	Identification and protection of an electronic security perimeter(s), within which all critical cyber assets reside.	1) All critical cyber assets to be included within an electronic security perimeter. 2) Implement and document access control for perimeter. 3) Monitor and log access to perimeter.

(continued)

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Table 6.1 (continued)
Proposed cybersecurity standards: CIP-002–CIP-009.

Reliability standard	Title	Purpose	Key requirements
CIP-006–1	Physical Security of Critical Cyber Assets	Creation of physical security program for critical cyber assets.	1) Implement physical security plan. 2) Control, monitor, and log physical access to critical cyber assets. 3) Test and maintain physical security systems at least once every three years.
CIP-007–1	Systems Security Management	Definition of methods, processes, and procedures for securing systems determined to be critical cyber assets.	1) Test all changes involving changes to critical cyber assets. 2) Disable all unused ports. 3) Use malicious software prevention programs and patch-management program. 4) Limit administrator access to critical cyber access. 5) Monitor systems for security breach. 6) Conduct annual cyber vulnerability assessment.
CIP-008–1	Incident Reporting and Response Planning	Identification, classification, response, and reporting of cybersecurity incidents.	1) Develop and implement incident response plan. 2) Document cybersecurity incidents.
CIP-009–1	Recovery Plans for Critical Cyber Assets	Development and implementation of recovery plans for critical cyber assets.	1) Create and annually review recovery plans. 2) Exercise plan annually. 3) Maintain backup information for successful restore of critical cyber assets.

Source: Proposed NERC CIP reliability standards collected in NERC, "Cyber Security: Standards CIP-002–1–CIP-009–1."

in a "Frequently Asked Questions" document submitted as part of its filing. In it, NERC noted that the phrase had a 200-year history in business and corporate common law and here was meant "to reflect—and to inform—any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards—that Responsible Entities have a significant degree of flexibility in implementing these Standards."[113] Historically, the principle protects corporate officers and board members from judicial review. Under the accepted legal meaning of this phrase, corporate board members and directors are granted wide discretion in their official capacity to act on behalf of the business, and they are obligated to act in what they perceive to be the best financial interests of the company.[114] Their decisions are protected from judicial review as long as they do not act with gross negligence. As NERC described:

> Courts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances. A common formulation indicates the business judgment of an entity—even if incorrect in hindsight—should not be overturned as long as it was made (1) in good faith (not an abuse or indiscretion), (2) without improper favor or bias, (3) using reasonably complete (if imperfect) information as available at the time of the decision, (4) based on a rational belief that the decision is in the entity's business interest.[115]

The principle of reasonable business judgment would, if included, plainly protect the autonomy of industry players to operate with wide discretion.[116]

The power industry argued that reasonable business judgment was an important part of the CIP standards. For NERC, Pacific Gas and Electric, San Diego Gas and Electric, and others the inclusion of this language would protect the right of regulated entities to weigh the presumed costs and benefits associated with any new security measure. In their estimation, security should be carefully considered within the broader scope of the costs and benefits to each individual company. Without such a qualification, they noted, new forms of security could be prohibitively expensive.[117] Likewise, Tampa Energy and Progress Energy and others asserted that the reasonable business judgment qualification was necessary to provide responsible entities the flexibility to implement CIP standards in ways best suited for their operating profile.[118]

FERC disagreed. The reasonable business judgment qualification was a significant problem. It would—if included—make a mockery of the very idea of mandatory standards. This language would allow regulated parties to disregard (so-called) mandatory reliability standards if, in their estimation, doing so conflicted or was unsupported by the financial best

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

interests of the company. Including this qualification would protect regulated parties from effective oversight; it would narrow the circumstances in which FERC and the courts could step in and review the actions of regulated parties.[119] For FERC, allowing individual firms wide discretion ignored an obvious tension: the pursuit of individual financial well-being and the overall security of the bulk power system do not always align. The CIP reliability standards sought (and seek) to promote the security of the interconnected electric power grid, not the best interests of any *single* company's shareholders.[120] As FERC remarked in reviewing NERC's proposal, "business convenience cannot excuse compliance with mandatory Reliability Standards."[121] Indeed, mandatory reliability standards were initially called for precisely because these two interests—parochial financial interests and security—often diverged. The interdependent nature of the power grid, and more specifically the ICTs and networks connecting different parties, rendered the reasonable business judgment standard particularly troubling.[122] Weak cybersecurity by one party involved in the bulk power system could undermine the security of other interconnected parties and the larger grid. As FERC noted, "Cyber standards are essential to protecting the Bulk-Power System against attacks by terrorists and others seeking to damage the grid. Because of the interconnected nature of the grid, an attack on one party can affect the entire grid."[123] In other words, the security of a system is only as strong as its weakest link.

FERC took aim at another provision in the CIP standards that would allow regulated players to effectively opt out of the regulations. A number of the initially proposed CIP standards included clauses that would have allowed regulated entities to issue a statement "accepting risk" in lieu of complying with the outlined requirements.[124] Multiple proposed standards included this "opt out" language.[125] For example, CIP-007 would have allowed parties to opt out of the requirements to close all unused ports (connections), adopt regular patches for known vulnerabilities involving critical cyber assets, or use antimalicious software protection.[126] If a party issued a statement accepting the risk in these cases, it would no longer be bound by the specific requirement of the standard.[127] In NERC's view, this provision allowed responsible parties to acknowledge the inevitable limitations of particular security strategies and investments.[128] Tampa Electric and Idaho Power joined NERC on similar grounds, supporting the provision. In their view, the elimination of all risk was neither possible nor, when costs were taken into account, necessarily desirable.[129] Industry sought these loopholes or exceptions as a way of maintaining their independence. FERC rejected these claims and strengthened its oversight

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

power. Regulators argued that the effectiveness of mandatory reliability standards could not be squared with allowing entities to opt out of key requirements at their own discretion.[130] As FERC remarked, there were "no controls or limits on a responsible entities use" of the acceptance of risk exception.[131] As it noted, FERC would have little power to review these sorts of enormously consequential decisions:

> A responsible entity may invoke the "acceptance of risk" exception without any explanation, mitigation efforts, evaluation of the potential ramifications of accepting the risk, or other accountability. In essence, the phrase "or an acceptance of risk" allows a responsible Entity to opt out of certain provisions of a mandatory Reliability Standard at its discretion.[132]

The acceptance of risks was not tempered by even a modest requirement calling on entities to justify or explain why they had chosen this decision. Deciding to accept a risk could be done for essentially any reason. Echoing its concerns regarding reasonable business judgment, FERC remarked that due to the "interconnected control systems of various entities, an acceptance of a cyber risk by one entity is actually an acceptance of risk for all of those connected entities because the entity that initially accepted the risk is now the weak link in the chain."[133] The acceptance of risk by one party, then, would have an impact on others. It would force all other interconnected parties to also accept this risk regardless of the wisdom of doing so.[134]

FERC's objections to the seemingly bland language that dotted the standards were important. Here, in the trenches of bureaucratic minutiae, the basic terms between the industry and the public and its proxies were being sorted out. For FERC, both the reasonable business judgement and the acceptance of risk provisions were traps: they turned mandatory standards into mere suggestions; they turned federal regulators into a staff of pliant observers; and they would make industry, essentially, beyond review. FERC fought back. It directed that these clauses must be struck from the next iteration of the CIP standards. Regulators offered a stern warning: if NERC did not comply, it would be fined and stripped of its status as an ERO, and FERC would find a different organization to serve as the industry steward.

Rewriting the Standards: Specificity and Penalties for Noncompliance

FERC worked to give the CIP standards real bite. During the initial review of the proposed standards, it became clear that federal regulators were not going to rubber-stamp whatever came across their desks. In addition to closing the various loopholes identified above, they also worked to make

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the standards more specific and the penalties for noncompliance meaningful. The first set of proposed CIP standards focused almost exclusively on general, vague outcomes at the expense of offering specific guidance concerning how to meet goals.[135] The regulations often amounted to little more than bookkeeping exercises. At the same time, the first slate of proposed penalties for violating the standards amounted to little more than a slap on the wrist and did little to encourage compliance. FERC flexed its power, and the standards were remade.

FERC and the industry had vastly different ideas about regulatory philosophy. For NERC, regulations would ideally specify outcomes and goals while deferring to the regulated parties on how to best meet those goals.[136] The CIP standards initially put forward general goals and left each individual entity to figure out *how* it might meet those goals.[137] For example, CIP-002 called for the use of "risk-based" methodology in developing cybersecurity plans. Yet the reliability standard offered no interpretation as to what such a methodology might entail.[138] FERC was leery. The lack of specificity made the standards little more than requirements to keep documents on file.[139] Of the 41 total requirements included within the initial slate of proposed CIP standards (each standard contained multiple requirements), *38* related to the mere possession of documents.[140] If these standards were adopted, FERC would have nothing to do except ensure that various documents were filed. It would lack any real power to review the substance of how regulated parties were confronting cybersecurity challenges.[141] FERC called for more concrete and binding standards. Without specific guidance, each entity could interpret the requirements as it wished and, in the process, undermine the interconnected bulk power system.[142]

FERC took issue with the proposed penalties attached to the draft standards. It was bad enough that the standards would, if adopted, allow regulated parties to pick and choose which standards to comply with. NERC also proposed paltry penalties for noncompliance. The penalties were set against a scale based on "violation risk factors." Each individual requirement and subrequirement of a mandatory reliability standard was assigned a corresponding violation risk factor. These factors were divided into three categories: lower, medium, or high.[143] These categories affixed the upper and lower limits of monetary penalties that could be assessed for infractions.[144] A high violation risk factor indicated that a violation of the requirement could directly contribute to or cause system instability and a cascading failure. A medium violation risk factor was reserved for requirements that, if violated, would affect the interconnected power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

system but be unlikely to lead to cascading failure or instability. Lower violation risk factors were assigned to requirements that were only administrative in nature: these types of violations were not expected to affect the capability of the bulk power system.[145] The fixed range of penalties differed significantly: infractions of lower violation risk factor requirements carried fines between $1,000 and $25,000, violations of medium-level requirements carried fines between $2,000 and $335,000, and violations of high-level requirements ran from $4,000 to $1 million.[146]

NERC initially labeled the overwhelming majority of the requirements in the CIP standards—85%—as "lower" violation risk factors.[147] It attempted to classify mandatory cybersecurity standards as little more than administrative requirements. NERC proposed a $25,000 cap for most penalties. Federal regulators balked. This, in their view, failed to recognize the seriousness of the challenges of cybersecurity.[148] For example, CIP-002 called for the identification and recording of all critical assets and critical cyber assets. This carried lower and medium violation risk factors, respectively.[149] Yet, as FERC noted, these requirements were not merely administrative: they controlled how, *or even if*, the larger family of reliability standards would apply. Failure to identify a critical asset or critical cyber asset would, in effect, fail to trigger *any* of the other CIP standards.[150] FERC pushed back and sought real penalties. The regulators called for increasing the severity of 43 of the 162 proposed violation risk factors.[151]

The Surprising Success of FERC

FERC changed the CIP standards in a meaningful way. The Energy Policy Act was supposed to help codify industry control. Indeed, the initial version of the standards proposed by industry was incredibly lax—it allowed industry to opt out of regulation as they saw fit, imposed few specific mandates, and carried only modest penalties. Outside observers viewed the standards as a significant failure.[152] Yet something surprising happened. The standards improved. FERC pushed back and chiseled out a space for the real, meaningful public review of electric power. The regulators did not accept the watered-down standards initially proposed, and they did not accept sitting on the sidelines approving whatever the industry cooked up. FERC approved the initial proposed standards but, at the same time, used its authority to direct NERC to make significant changes and resubmit a new version of the standards for review. It was not an idle request. If NERC failed to develop standards that responded to FERC's specific concerns, FERC would strip NERC of its power. It was a serious penalty: removal of NERC as the ERO. FERC's demands were met. In the next

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

iteration of standards proposed by NERC—CIP version 2.0—the reasonable business judgment and accept the risk provisions were eliminated, the CIP standards became more specific, and the penalties were increased for 43 different types of violations.[153] This pattern has now repeated. Through multiple revisions—FERC approved the sixth version of the CIP standards in 2016—FERC has used its power to greatly alter and improve the CIP standards.[154] Although it cannot draft new regulations, FERC found a way to hold the pen. Taken together, FERC transformed the proposed mandatory reliability standards from vague administrative standards containing multiple avenues for opting out into something far closer to comprehensive regulations. The regulators have held industry to account.

Public Accountability and Security

The development of the first mandatory cybersecurity regulations for the electric power system is an interesting case. These new interventions confront the contradictions of deregulation. The move toward competitive markets inadvertently introduced new forms of vulnerability into the bulk power system. After the blackout of 2003, experts reviewing the bulk power system underscored the need to create mandatory cybersecurity standards to confront the threat of terrorism and intentional disruption. The tension between security and the market became an acute problem.

The Energy Policy Act of 2005 outlined what were basically conservative responses to these problems. It appeared, at first blush, to be little more than the retrenchment of the ethos of deregulation. It put in place measures that would—or at least seemed to—enhance the power of industry. The complex standards process that followed the act was designed to allow industry to self-police with little oversight from federal regulators or the public. Industry, it seemed, would have far greater power to control the terms upon which electric power operated, while other infrastructure publics would be shut out. Yet the development of mandatory regulations took an unexpected turn. FERC transformed the seemingly thin powers it was left with and carved out a significant role for expanded federal—that is, public—oversight of electric power. FERC expanded its power during the initial approval of NERC as the ERO—giving it more power to oversee and define *all reliability* standards moving forward. In time, this affected not just those standards related to cybersecurity but a larger set of standards related to emergency preparedness, facility design, interchange scheduling and coordination, and other topics. FERC put its power to use during the approval and review of the CIP reliability

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

standards and successfully transformed what were lax regulations into tight controls. Federal regulators took seriously the prioritization of security and followed through to a reasonable conclusion: tough standards were needed. FERC seized on the ambiguity within the Energy Policy Act's call for federal review in the public interest, on the one hand, and its stated preference for deference to the desires and judgment of industry, on the other. It offered an aggressive interpretation of the scope of federal power. Rather than simply enforcing industry-approved provisions, federal regulators took their role to review proposed standards seriously and directly challenged industry preferences in a meaningful way. New legislation designed to give industry broad power was reinterpreted by federal regulators to support robust public accountability. There is an important, if familiar, lesson here: once on the books, agencies and the public can spin regulatory authority in surprising ways.

The creation and implementation of mandatory cybersecurity reliability standards was a battle to determine authorship over new regulatory controls. How the uncertain threat of terrorism and an expanded notion of security would be translated into routine and standard practices was an open question that pitted industry and federal regulators against each other. FERC's success ensures that there will be meaningful public review of how electric power companies operate. New forms of public accountability have been created. The establishment of a substantial role for FERC in overseeing regulatory standards is a significant victory for the public. Robust FERC review ensures that electric power will be held to account by public institutions—electric power companies must justify and balance their interests against a larger set of concerns. Likewise, FERC's process of regulatory review ensures transparent decision-making and ample opportunities for comment from diverse stakeholders: it creates a durable forum through which different infrastructure publics can both access information about electric power and have their voices heard. The regulatory process opens the workings of electric power to public discussion and review. This is not trivial: the work of FERC's regulators to reassert themselves within electric power leads both to better security controls and, importantly, a recalibration of the social relations that define the electric power system. Deregulation, at its core, attempted to close infrastructures to public scrutiny and accountability. It greatly diminished the role that public institutions play in overseeing infrastructures in deference to the market. Here, through the guise of security, the workings of the infrastructure are pried open with a snap, and the public is let back in.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Conclusion: The Politics of Critical Infrastructure Protection

The recasting of infrastructures as dangerous things was—and *is*—potent. It created a moment of political reflexivity, an opportunity to revisit and reorder the material and organizational foundations of infrastructure. *Infrastructures always order*: they inevitably prioritize certain users, certain uses, and particular visions of these systems over others. Security offered a way to alter how different infrastructure publics—particular customers, operators, regulators, advocacy groups, and others—relate to one another. It promised a reconsideration of which publics, uses, and imaginings of infrastructure would be prioritized and which would be marginalized.

The postal system, the freight rail network, and the electric power system have each been transformed. Additional layers of security technologies, regulations, standards, and practices now govern these systems. Once novel and contentious, these practices have become a regular and largely taken-for-granted part of these infrastructures. These changes are dramatic and uneven: dramatic in the sense that they sprang from high-stakes and deeply contested battles between various infrastructure publics, and uneven in that the outcomes of these dramas, these fights, are ultimately mixed. The reframing of these systems as dangerous things allowed for the larger set of political choices built into these systems to become visible and open to debate. Decades of political and economic reform—deregulation—pushed these systems to the brink. It stripped away key mechanisms of public oversight *and* created new forms of systemic vulnerability at the core of these networks. The recasting of infrastructures as dangerous things created real possibilities for change. It offered the chance to reckon with the consequences of deregulation. It offered the opportunity to revisit and remake the status quo. It offered the chance to shift power within these systems. It offered the opportunity to address the material vulnerabilities that sat at the center of these infrastructures. The

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

complex transformation of infrastructures into dangerous things after 9/11 offered (and might still offer) this and more. It offered possibilities. *Possibilities*. Not certainties.

The refashioning of the postal system, freight rail network, and electric power grid followed two very different paths. In freight rail and electric power, something surprising happened. New security practices reordered power within these networks. Groups that had been pushed to the margins found in the post-9/11 vernacular a new voice and a new way of organizing. New regulatory powers, rules, and practices now provide a degree of public accountability that had withered or gone missing. These changes are at odds with how we most often think about post-9/11 security politics. Security concerns in these cases did not feed increased secrecy; they did not lead to the further consolidation of power in the hands of the few; they did not lead to the erosion of democratic norms; and they did not lead to ineffective security theater. They led to new forms of public accountability. The adopted regulations check the power of incumbents and key customers to control infrastructure. They are a counterweight. The now-in-place regulatory powers offer the opportunity for public officials to scrutinize, review, and push back against decisions made by influential corners of industry and, importantly, they provide an opportunity for *other* infrastructure publics to do the same. The regulatory process is open. It invites comment and review from a diverse array of players. Powerful electric power companies or railroads cannot simply set their own rules. They are pushed into dialogue with other publics whether they like it or not. The adopted regulations enable public accountability because they allow multiple competing publics an opportunity to examine how core infrastructure operators work; they acknowledge the plural publics that are bound together through infrastructure; they offer a venue for different publics to advocate for their interests; and they embrace a logic—a way of interpreting and making decisions about how infrastructures *should* operate—that is open to competing values and interests and not simply subservient to the demands of the market.

These changes are not just smart politics that are laudable for their inclusive bent. They also address the material vulnerabilities that decades of political and economic reform helped to create. In freight rail, the adopted changes reduce the risks associated with the transportation of dangerous cargoes. Decades of political and economic reform encouraged bulk shipments of hazardous materials along the most cost-efficient routes possible, bringing them through cities and tightly packed areas. This generated real risks. This type of *spatial dependency*, fusing together

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the city and the transportation of bulk shipments of hazardous materials, creates the potential for catastrophic releases.[1] The adopted security regulations work to break these connections by pushing bulk shipments away from populated areas. This is a significant reversal. Security regulations force rail companies to consider something other than the bottom line in making routing decisions. The story in electric power is very much the same. The Critical Infrastructure Protection (CIP) standards address serious risks in a useful way. The evolving CIP standards work to limit the vulnerabilities related to the integration of generative networked computers within electric power. Deregulation hastened the adoption of this particular model of computing and networking, while also binding together power systems into larger configurations. The CIP standards push back. They work to isolate or segment operational technology from other larger multipurpose networks and require companies to inventory their assets and adopt limits and controls on how they might be used. These standards cannot turn back the clock to the world of single-purpose machines and dedicated networks. But they do work to reduce risk. The splintering of power within these infrastructures—bringing many different publics back in—improves security.

The rail and electric power cases paint a rosy picture of how infrastructure fears, backed by a set of supporting institutional changes and stout organizational advocacy, can translate into new forms of public accountability that carry both political and security benefits. The case of the postal system tells a different story. Here, power is not reordered: existing hierarchies are further entrenched. The aftermath of the anthrax attacks for a moment appeared to offer postal workers the chance to seize new powers to dictate postal policy. Suddenly on the "front lines of the war on terror," labor challenged the power of commercial mailers to define postal policy and sought security solutions that would protect them from harm. But the hopes of workers were dashed. Any sort of larger transformation was ultimately fleeting: new forms of security did not upend the status quo. On the contrary, security practices cement the prominent position of a cadre of commercial mailers at the expense of postal workers. The Biohazard Detection System (BDS) and Intelligent Mail program serve the interests of large commercial mailers. The benefits of these systems are partial. The health and safety of workers are traded away in favor of lower costs for bulk mailers, new tools engineered to help aid the adoption of temporary noncareer (nonunion) workers, and new, informational postal products pitched to industrial customers. Postal employees might have been able to claim they were on the front

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

lines of the war on terror, but new forms of infrastructure security are more worried about the bottom line of commercial mailers than the well-being of workers. The recasting of infrastructures as dangerous things is ripe with the potential for change. But, as the collected cases make plain, the shape and form these changes can take are very much open.

What are we to make of these contradictory changes? These vignettes complicate our understanding of post-9/11 security politics and the political power of risk. These cases do not necessarily fit the usual or familiar ways in which we think about or understand the politics of infrastructure security. These cases are not, in the main, stories about security theater. Nor are they only stories about how already powerful groups—government or industry—use catastrophes to enhance their already substantial powers. These cases offer a different picture. The risk of terrorism became a powerful rallying cry that served multiple ends. Marginalized groups used it to reckon with the consequences of decades of political and economic reforms. Fears about these dangerous things were translated into new forms of public accountability. These changes address real systemic vulnerabilities and reorder power. They open infrastructure to different publics. New forms of security, in the cases of freight rail and electric power, are something of a restoration. Decades of political and economic reforms removed the key mechanisms that provided public oversight of infrastructure. Now, oversight is reinvigorated in the guise of security. Yet sitting side-by-side with stories about the transformative power of risk is the case of the postal system. Sometimes risks *do* serve the powerful. Sometimes fears are translated into practices and tools that further entrench the powerful. Sometimes the familiar story also happens to be true. Taken together, these cases are fragments that complicate our understanding about the contradictory post-9/11 world that we still are living in, and they remind us that risks are unruly fissures that can run in multiple directions.

* * * *

Case studies are always partial glimpses into a larger world. They tell us something specific and, in doing so, point toward something larger. Shifting through these cases reveals larger themes and observations. These insights can help plot a path forward. The recasting of infrastructures as dangerous things remains very much alive. The threaded cultural, institutional, and organizational changes that came to the fore in the years after the terrorist attacks of September 11 and transformed infrastructures into dangerous things are still in place. The long shadow of

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

9/11 continues—nearly two decades later—to color how we think about, interact with, and make and remake infrastructure. The case studies offer insights that can be used to navigate and make sense of the politics of infrastructure security. Three key insights stand out.

Recovering the Sunk Politics of Infrastructure: The Importance of Historical Thinking

Infrastructures are monuments to the past. Contingent choices made decades ago become ossified within the inner workings of these systems. Decisions that are wise, foolish, or simply the product of happenstance can and often do reverberate within these systems for decades in subtle and explicit ways. It is easy to lose sight of the histories encoded within these systems. Forgetting is perilous. It makes it difficult to clearly understand the stakes that cling to contemporary infrastructure security interventions.

In each of the cases collected in these pages, choices made during the last third of the 20th century set the stage for the conflicts over infrastructure security that would arise at the start of the 21st century. Deregulation was a thorough transformation of the postal system, freight rail network, and electric power grid. The political and economic project of deregulation became distilled within each of these systems. The adoption of new centralized automated facilities in the postal system, the spike in hazardous materials carried by rail, and the integration of networked generative computers within electric power were each, in different ways, products of deregulation. These changes were not inevitable: they were the intended and unintended consequences of political choices. Political and economic reform was not simply contemporaneous with the adoption of automated postal machines or multipurpose computers within electric power: reforms drove the adoption and integration of certain technical components and elements within the larger network assemblage. The shifting mix of commodities handled by the railroads during the 1980s and beyond was not the product of immutable laws of economics: it was the product of legislative changes and related regulatory decisions about how to assign costs and markups. Political choices were reproduced within these networks in subtle (and not so subtle) ways. Later—but only later—these changes would become legible as the key drivers of systemic vulnerability. That is, they would become problems that needed to be fixed.

Individual infrastructure components embalm the past and carry it into the present. Identifying the role that larger historical forces play in shaping the material outlines of infrastructure is vital. It is more than just

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

understanding how or why a particular facet of a system came to be—it is a necessary element for sorting out the stakes of contemporary security conflicts. In the cases examined, drawing a thick line connecting deregulation and post-9/11 security efforts points out a core structural tension: the seeming incompatibility between the drive for increasingly efficient infrastructures under private control and the desire for secure systems. Identifying and understanding this tension is important. It crystallizes the larger ideological stakes and conflicts sitting beneath the surface. The documented security efforts cataloged here constantly run up against the thrust of the larger political and economic project of deregulation. Post-9/11 debates about infrastructure security were implicit and explicit referendums on deregulation. The overlooked costs of political and economic reforms came due. Recapturing the history sunk within these systems offers a reminder that infrastructure security is always about more than tinkering with the settings on a workstation at an electric power company, it is about more than figuring out what particular route a train hauling chlorine should take, and it is about more than determining which piece of automated sorting equipment should have an "anthrax smoke alarm" (as the BDS is sometimes known). It is about grappling with the collision between the politics of the past that have become encoded and drilled into the workings of infrastructure and the fast-moving onrush of the politics of the moment that seek to remake and revisit these systems.

Historicizing infrastructure uncovers the tension between the politics of the past and present. It draws out the larger ideological conflicts and political choices that sit behind security debates. The cases here looked at the tension between post-9/11 security anxieties and deregulation and revealed a rich irony: decades of promarket infrastructure reforms led to the need for increasingly intense state interventions to stabilize these systems. Future cases examining infrastructure security in various contexts will find surprising collisions between past and present. Historicizing infrastructure security underlines and makes visible the larger structural tensions that are at play. It offers a window into why efforts to remake infrastructures and bolt on new forms of security can be difficult and face stiff opposition. It provides a glimpse into how distinct political moments collide. In other words, it starts to clarify what exactly is at stake when infrastructures are made secure.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Infrastructure Orders: Infrastructure Publics and Their Problems

In focusing on infrastructure security interventions and efforts, the question "Do they work?" *must* give way to the larger question "For whom do they work?" Torin Monahan first proposed a similar reframing as a way of understanding and critiquing surveillance.[2] But this insight is just as relevant when applied to infrastructure security. Thinking through the practical impacts of security efforts—whether they succeed or fail in making systems more or less secure—*cannot* be disentangled from a larger reckoning with how security practices produce particular types of social relations. What counts as "secure" is always negotiated and provisional. It only emerges through the clash of battling infrastructure publics and competing visions about for what and for whom these systems are made.

In the wake of the 2001 anthrax attacks, a sharp contest between commercial mailers, labor, and management broke out. Each of these groups had its own priorities and saw security differently: commercial mailers wanted to reassure the public that the mail was safe while limiting any additional costs or delays to the mail; labor wanted a safe workplace and a greater say in postal policy, particularly as it related to how new technologies would be integrated into the mail system; and management wanted to keep the postal system viable in the face of its myriad economic woes and quell the bubbling panic from the attacks. These and other players wanted to create a secure system, but what that meant for each group did not always align. Each group related to the postal system differently. For letter carriers and clerks, the postal system was where they worked. It was a job. For commercial mailers it was a cheap, low-cost network that links advertisers with consumers. The postal system means different things to different publics. It is unsurprising, then, that what constituted a "secure" system also diverged for these groups.

Infrastructures create and bind together different publics. They fuse heterogeneous publics into a tentative hierarchy. Certain publics—as well as uses and infrastructural imaginings—are prioritized, while others are shoved aside. New security efforts invariably offer an opportunity to maintain or reshuffle these orders. They offer a chance to reconsider what publics matter, which visions count, and what uses are given priority over others. Security efforts order these publics, these visions, and these uses. They present different ways of arranging or prioritizing. Purely utilitarian frames—asking new security interventions such as "Do they work?"—elide too much: they ignore the different competing publics, meanings, and uses that are always contained and constrained within infrastructure.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Explorations of infrastructure security must be attuned to how security orders. The question "For whom do they work?" can usefully start this process. It places the multiplicity of infrastructure publics at the center of analysis and can reveal how producing a secure system is always about creating and affirming hierarchies.

The Promiscuous Politics of Security: Reflexive Modernization and the Power of Organized Interests

The case studies offer a reminder that risks are powerful *and* promiscuous resources. After the terrorist attacks of September 11, a number of key changes worked to transform infrastructures into dangerous things. President George W. Bush's framing of civilian infrastructure writ large as sites of danger and geostrategic security concern led an important cultural shift. This framing had circulated for decades during the Cold War and immediate post–Cold War era within think tanks and inside-the-Beltway policy circles. But the president's adoption of this frame gave it a new currency and legitimacy. Now it became acceptable and common to speak about infrastructure as targets-in-waiting. At the same time, the institutionalization of *critical infrastructure* security as a key priority through the creation of the Department of Homeland Security, the opening of spigots of federal and state funding devoted to this issue, and other changes ensured that this cultural reframing would become durable and powerful. This recasting, however, was not yet complete without the work of organized interests. Postal workers, environmental groups, electric utilities, and many others picked up on this framing and advocated for specific policies and practices. These changes—cultural, institutional, and organizational—transformed infrastructures into dangerous things. Deregulation may have created or enlarged systemic vulnerabilities, but these changes made these instabilities culturally and politically legible.

The collected cases paint an unfamiliar and contradictory picture of post-9/11 politics. The case of freight rail and electric power demonstrate how risks can serve as powerful catalysts for surprising political transformations and reversals. Typically, the politics of national security are taken to be antithetical to accountability and democratization. Security is often seen to be a trump card that can be used to extend the influence of the powerful; it is used to suspend normal democratic processes and, in their place, support exceptional powers. The cases in this book offer a more complicated portrait. In the cases of rail and electric power, the risk of terrorism was used to wrench open previously closed domains. Fears

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

over terrorism offered marginalized infrastructure publics a way to reassert their interests. Terrorism provided a scaffolding to build new forms of accountability that accommodated multiple different publics. In the postal case, as noted above, this did not happen. Here, a more familiar story unfolded: powerful players enhanced and extended their power.

These cases offer a reminder: risks are powerful, but promiscuous. They are always open to multiple competing interpretations. They can aid the powerful and the marginalized alike. Risks can create moments of instability, but how these moments are fashioned into lasting changes—the bureaucratization of risk—is always an open question. Investigations into infrastructure security must account for this promiscuity. Detailed empirical investigations into how organized interests work within a particular cultural and institutional milieu to harness the power and possibilities of risk are crucial. The preceding chapters provide an example of this type of study, mapping how moments of instability are first created and then fashioned into transformative or reactionary changes.

The Politics of Infrastructure Security

Infrastructures remain dangerous things. The particular set of cultural, institutional, and organizational changes set in motion after September 11, 2001, remains firmly in place. It is a powerful matrix. Security remains one of the primary ways in which we think about and shape infrastructure. The full implications of this recasting continue to unfold.

In the summer of 2018, President Trump held a rally in West Virginia. During his remarks, he offered a broad attack against renewable energy, stating: "In times of war, in times of conflict, you can blow up those windmills. They fall down real quick. … You can do a lot of things to solar panels, but you know what you can't hurt? Coal. You can do whatever you want to coal."[3] The symbolic use of national security—the language of war and conflict—to support a political priority is not new. President Trump's use of this trope to support coal—during a political rally deep in coal country—is not remarkable. Presidents freighted their causes with urgency by linking them to wars both real and metaphorical long before President Trump took office. But the weight and power of Trump's rhetorical invocation is different today than it would have been just two decades ago. The changes that followed September 11, 2001, make these sorts of calls powerful, regardless if they are justified or not. Here, Trump seemed to employ, in an offhand and difficult to parse manner, the language of national security to undermine support and investment in green

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

energy. This remark carries weight not just because the president uttered it but because there are now corresponding bureaucratic apparatuses (and billions of dollars) in place that support decisions about infrastructure based on notions of security that are elastic and fungible.

The relative "openness" of security makes it a powerful tool. It can be repurposed by different groups for varied ends. The idea that infrastructures are dangerous things sitting at the center of larger geostrategic conflicts remains salient. Infrastructure protection is now embedded within a web of institutions that are devoted to and prop up this idea. What remains to be seen is how organized interests will work within this terrain to advocate for new infrastructure orders. As the preceding pages make clear, security can be used to open infrastructures to multiple publics and different visions. It can be used to make infrastructures accountable to the various publics they create and bind. Or, invocations of security can be used as a tool to further marginalize: to seal off infrastructures to all but the most powerful voices; to elevate and embrace narrow sets of interests and imaginings of what these systems are for and whom they should serve. In other words, the recasting of infrastructures as dangerous things can be used to tear down walls or prop them up. The path that new and not yet waged battles over infrastructure security might take in the future remains undecided. Documenting how the powerful new cultural, institutional, and organizational context that surrounds infrastructure is translated into practice remains an ongoing task. The assembled case studies not only reveal the important changes and conflicts that mark these particular infrastructures but also offer a guide to an uncertain future and the infrastructural changes yet to come.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Coda: Infrastructure as Target

The book ends right where it began: with Director of National Intelligence James Clapper's public testimony before the Senate Select Committee on Intelligence in March 2013. Clapper's testimony became infamous. Not because of the prioritization of infrastructure security that his testimony marked, but for an exchange with Senator Ron Wyden.

Senator Wyden asked Clapper: "Does the NSA [National Security Agency] collect any type of data at all on millions or hundreds of millions of Americans?"

Clapper responded: "No, sir."[1]

A few months later, this terse exchange would come under close scrutiny. In June, stories started appearing in the *Guardian* (UK) newspaper and other outlets across the globe that revealed intimate details about the United States spying apparatus.[2] NSA contractor Edward Snowden had made off with a trove of classified files that provided a glimpse into the innermost workings of the secret spying bureaucracy. The first story drawn from the Snowden leaks revealed a government order requiring Verizon to turn over phone records related to tens of millions of Americans.[3] Clapper's comments appeared in a new light. Senator Wyden later charged that Clapper's statement was baldly false and misleading. Clapper claimed that given the constraints imposed by secrecy, his answer during the public hearing had been "the least untruthful" he could provide.[4]

The *Guardian*'s phone records story was the start of a flood. The leaked documents led to story after story detailing the work of the nation's most secretive intelligence agency. The code names appeared to be straight out of a spy novel. *Bullrun*. *Mystic*. *Boundless Informant*. *Prism*. These and other previously confidential programs were discussed and picked over in public for the first time. The picture that emerged put a new spin on post-9/11 debates about infrastructure security. While most, if not all, of those earlier debates had been about protection—how to secure the vital systems

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and networks that the nation relies on—under the cloak of secrecy a different set of efforts was unfolding. These newly revealed efforts were not about defense: they were about offense. The Snowden files revealed a well-financed and sprawling attempt to subvert and infiltrate digital infrastructures across the globe.

Reporting based on the leaked files revealed that the U.S. had worked to undermine encryption standards and products used worldwide. Encryption is a fundamental part of digital life. It is used to protect everything from private chats to online purchases (and a great deal more). News reports indicate that the NSA tried to undermine encryption in a number of ways, including inserting vulnerabilities into products, working with commercial vendors to encourage the adoption of weak standards that could be defeated via secret means, and interdicting and physically altering hardware.[5] The NSA reportedly spent $250 million a year to covertly influence companies to adopt designs it then could break.[6] The NSA also worked to purchase previously unknown and undisclosed software flaws—known as *zero-days*—from contractors. Zero-days are bugs that are not yet known to vendors—patches and updates are not available to mitigate these vulnerabilities. Hacking tools built on zero-days are both difficult to detect and to block.[7] According to reports linked to the Snowden documents, the NSA spent $25 million purchasing zero-days during a single year.[8]

While the U.S. government was spending billions of dollars on homeland security and prioritizing cybersecurity for critical infrastructure, it was at the same time developing policies, techniques, and technologies that undermine infrastructure security.[9] These efforts are not easily isolated.[10] The software, standards, and hardware that the NSA targets and penetrates are not only used by foreign spies, governments, and terrorists. The same technology is used inside the U.S.—by defense contractors, electric power companies, newspapers, hospitals, and ordinary users. As Bruce Schneier points out: "Because everyone uses the same software, hardware, and networking protocols, there is no way to simultaneously secure our systems while attacking their systems—whoever 'they' are."[11] Efforts targeting adversary networks can undermine U.S. interests and security. Weak encryption standards and unpatched flaws do not just mean that the U.S. can subvert foreign networks and gain valuable intelligence; it also means that U.S. companies, public-sector entities, and the everyday users that rely on these standards are also vulnerable to attack. Nothing prevents a different spy agency from finding these flaws and working to develop its own assault. It is something of a zero-sum game. As Schneier puts it: "Either everyone is more secure, or everyone is more vulnerable."[12]

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

The problem is complicated. The U.S. wants infrastructure security, and it also wants to collect valuable intelligence from its adversaries (and, in some cases, reserve the ability to launch attacks) at the same time. There is no simple way to untie this knot.[13] In order to ensure their own security, states will hack other states to glean important information. But this creates risks, such as inadvertent or accidental escalation. A hacking operation used to collect information might lead the target, through misunderstanding or aggravation, to respond with a more destructive move than anticipated.[14] Additionally, state-sponsored hacking campaigns risk legitimizing cyber operations, giving other countries and actors a green light to use malicious tools in new, potentially destructive ways.[15] But the use of offensive hacking tools carries another risk: the possibility or appropriation and reuse. The creation and use of these exploits and attacks might be turned back against their master.[16] The diffusion of common protocols, standards, and technology make offensive maneuvers a fraught proposition. The themes of this book now slide back into view. Decades of political and economic changes have privileged efficiency and free markets above all else. This helped drive the adoption of standard computing equipment over custom-built components in electric power. A similar story unfolded in other industries and within government. The adoption of cheap common components ties the world together in new ways—it creates a shared infrastructural public. Common software and hardware are now spread across infrastructures, making it difficult to spy on or attack adversaries without creating opportunities for them to do the same in return. A strong offense can undermine *your own* defense—while the development of a strong defensive posture can reduce *your own* ability to wage offensive campaigns.

These concerns are not idle. In 2016 a group calling themselves the Shadow Brokers appeared online.[17] They advertised what they called *cyber weapons*—tools and exploits stolen from the NSA.[18] The group, widely thought to be a front for Russian operatives, had the goods. They initially leaked exploits that targeted various network security systems.[19] Subsequent leaks made it clear that they had captured some of the NSA's most sensitive tools.[20] The Shadow Brokers were, in effect, doxing the NSA. The fallout was significant and showed the difficulties of creating offensive tools in a world that runs on shared technology. Once the tools had been publicly released, they were picked up and repurposed by various adversaries, to great effect.[21] WannaCry, a ransomware campaign built from one of these tools, spread across the globe and appeared in over 70 different countries. It was a reworking of a tool the NSA had created—named

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

EternalBlue—that took advantage of a flaw in Windows (the flaw is also known as EternalBlue). Microsoft had released an update to fix the flaw weeks before, but many machines remained unpatched and vulnerable.[22] WannaCry spread quickly. It hobbled the National Health Service in the UK, holding computers ransom unless its victims paid up. It affected railways, schools, and other infrastructure sectors.[23] WannaCry was not trivial. It led to between $4 billion and $8 billion in damages.[24] But things would get worse. A month after WannaCry, a new worm that also modified EternalBlue—named NotPetya—wreaked havoc. It spread first through Ukraine and then found its way into machines across the globe. As journalist Andy Greenberg's detailed rendering of the incident accounts, NotPetya affected a French construction company, a hospital in Pennsylvania, the drug company Merck, and, maybe most notably, Maersk, the world's largest container-shipping company.[25] In a flash, corporate computers and networks were rendered useless. The harm was significant. The White House estimated the total costs associated with NotPetya at $10 billion.[26] For years, observers inside and outside of government had worried that the development of offensive capabilities might boomerang and come back to haunt the U.S. Now it had.

Infrastructure security always calls for a reckoning with larger values. It asks which publics and which visions of a system *matter*. Security codifies a particular way of ordering. The ongoing development of offensive cyber capabilities may be necessary—but it is certainly fraught. It collides with the massive investment in infrastructure security that the U.S. has committed since 9/11. Sorting out this conflict—between defense and offense in a world stitched together with shared code—is an ongoing and open question. It echoes across debates about encryption policy, debates about the purchase and use of zero-day vulnerabilities, and other areas and conflicts involving state-backed hacking operations. Like the post-9/11 battles cataloged in this book, these debates will be sorted out through conflicts between competing infrastructural publics. The stakes remain high.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Notes

Introduction

1. *Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Select Committee on Intelligence* (statement of James Clapper, Director of National Intelligence), March 12, 2013, https://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/816-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-intelligence-community.

2. Video of Clapper's appearance before the Senate Select Committee on Intelligence is available online: Senate Select Committee on Intelligence, March 12, 2013, https://www.c-span.org/video/?311436-1/senate-intelligence-cmte-hearing-worldwide-threats-us; James Clapper, *Remarks as Delivered, Worldwide Threat Assessment*, Senate Select Committee on Intelligence, March 12, 2013, https://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf.

3. Ibid.

4. *Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community* (James Clapper).

5. Ibid.

6. Ibid.

7. Mariano-Florentino Cuéllar, *Governing Security: The Hidden Origins of American Security Agencies* (Stanford, CA: Stanford Law Books, 2013), 127.

8. *National Security Strategy of the United States* (Washington, DC: Government Printing Office, 2017).

9. U.S. General Accounting Office (GAO), *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02–474 (Washington, DC: GAO, 2002), 27.

10. John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, prepared by the Congressional Research Service (Washington, DC: Library of Congress, 2003), 32.

11. Figures tabulated from the U.S. Office of Management and Budget, "Appendix: Homeland Security Mission Funding by Agency and Budget Account," in

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Analytic Perspectives: Budget of the U.S. Government: Fiscal Year 2017 (Washington, DC: Government Printing Office, 2016).

12. Ibid.

13. Ibid.

14. Lisa Benton-Short, *The National Mall: No Ordinary Public Space* (Toronto: University of Toronto Press, 2016); Martin Kaste, "Thanks to Sept. 11 Security 'Inertia,' Restrictions Still Shape Public Spaces," *NPR,* September 11, 2016, http://www.npr.org/2016/09/11/493292448/thanks-to-sept-11-security-inertia-restrictions-still-shape-public-spaces; Anthony DePalma, "Security Planters: Hard Reminders of Stark Realities," *New York Times*, June 7, 2005.

15. U.S. Department of Homeland Security, *Privacy Impact Assessment Update for TSA Advanced Imaging Technology*, December 18, 2015, https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf; Massport, "Security Information," n.d., http://www.massport.com/logan-airport/at-the-airport/security-information.

16. Hanson O'Haver, "How 'If You See Something, Say Something' Became Our National Motto," *Washington Post*, September 23, 2016.

17. Manny Fernandez, "A Phrase for Safety after 9/11 Goes Global," *New York Times*, May 10, 2010.

18. For a detailed discussion, see chapter 4.

19. U.S. Department of Homeland Security, *Privacy Impact Assessment Update for the Enhanced Cybersecurity Services (ECS)*, November 20, 2015, https://www.dhs.gov/sites/default/files/publications/privacy-pia-28-a-nppd-ecs-november2015.pdf.

20. National Science and Technology Council, *Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations* (Washington, DC, 2008), 34–35, https://fas.org/irp/eprint/biometrics.pdf; Ronald D. White, "Port Security Goes from an Afterthought to a Priority," *Los Angeles Times*, September 9, 2011.

21. Paul Edwards, "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems," in *Modernity and Technology*, ed. Thomas J. Misa, Philip Brey, and Andrew Feenberg (Cambridge, MA: MIT Press, 2003), 185.

22. See Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven, CT: Yale University Press, 2018).

23. This is a reworking of Torin Monahan's framing of how to approach questions concerning surveillance. Torin Monahan, "Questioning Surveillance and Security," in *Surveillance and Security: Technological Politics and Power in Everyday Life*, ed. Torin Monahan (New York: Routledge, 2006), 1–26.

24. The choice of *publics*—plural—is deliberate: it highlights the ways in which infrastructures construct and impact different communities in different ways. More generally, the public is always comprised of multiple publics. On infrastructure publics, see Stephen J. Collier, James Christopher Mizes, and Antina

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Von Schnitzler, "Preface: Public Infrastructures/Infrastructural Publics," *Limn*, no. 7 (July 2006); Christopher A. Le Dantec and Carl DiSalvo, "Infrastructure and the Formation of Publics in Participatory Design," *Social Studies of Science* 43 no. 2 (2013): 241-264. On publics more generally see John Dewey, *The Public and Its Problems: An Essay in Political Inquiry* (New York: Henry Holt, 1927).

25. Bruce Schneier, "Beyond Security Theater," *Schneier on Security*, November 2009, https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html; Bruce Schneier, "In Praise of Security Theater," *Schneier on Security*, January 2007, https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html.

26. For example, see Stephen Graham, *Cities under Siege: The New Military Urbanism* (Brooklyn: Verso, 2011); Stephen Graham, ed., *Cities, War, and Terrorism: Towards an Urban Geopolitics* (Malden, MA: Blackwell, 2004).

27. On disaster capitalism, see Naomi Klein, *Shock Doctrine: The Rise of Disaster Capitalism* (New York: Metropolitan/Holt, 2007); Anthony Lowenstein, *Disaster Capitalism: Making a Killing Out of Catastrophe* (New York: Verso, 2015).

28. Robert B. Horwitz, *The Irony of Regulatory Reform: The Deregulation of American Telecommunications* (New York: Oxford University Press, 1989).

29. Tony Judt, *Ill Fares the Land* (New York: Penguin, 2010).

30. Charles Perrow, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (Princeton, NJ: Princeton University Press, 2007); Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (1984; repr., Princeton, NJ: Princeton University Press, 1999).

31. Claudia Aradau, "Security That Matters: Critical Infrastructure and Objects of Protection," *Security Dialogue* 41.5 (2010): 491–514.

32. See Laura K. Donohue, *The Cost of Counterterrorism: Power, Politics, and Liberty* (New York: Cambridge University Press, 2008); Charlie Savage, *Takeover: The Return of the Imperial Presidency* (New York: Back Bay Books, 2007); Charlie Savage, *Power Wars: Inside Obama's Post-9/11 Presidency* (New York: Little, Brown, 2015).

33. Mark Danner, "After September 11: Our State of Exception," *New York Review of Books,* October 13, 2011.

34. Ibid.

35. Graham, *Cities under Siege*.

36. See Graham, ed., *Cities, War, and Terrorism*; Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Malden, MA: Polity, 2013); David Lyon, *Surveillance after September 11* (Malden, MA: Polity, 2003).

37. This insight follows Jack Goldsmith's similar argument concerning executive power, the war on terror, and accountability. Goldsmith, *Power and Constraint: The Accountable Presidency after 9/11* (New York: Norton, 2012).

38. Langdon Winner, "Techne and Politeia," in *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: University of Chicago Press, 1989), 40–60.

39. Giorgio Agamben, *State of Exception*, trans. Kevin Attell (Chicago: University of Chicago Press, 2003).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

40. Cuéllar, *Governing Security.*

41. Ibid., 191.

42. Ibid., 211.

43. Ulrich Beck, *Risk Society: Towards a New Modernity*, trans. Mark Ritter (Thousand Oaks, CA: Sage, 1992).

44. Geoffrey C. Bowker, Karen Baker, Florence Millerand, and David Ribes, "Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment," in *International Handbook of Internet Research*, ed. J. Hunsinger, L. Klastrup, and M. Allen (Dordrecht, The Netherlands: Springer, 2009), 97–117.

45. Barack Obama, Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

46. Thomas P. Hughes' discussion of the development of electric power systems argues forcefully for an expansive notion of technological systems. Using electric power as his point of departure, he investigates the relationship between technical artifacts, organizations, regulations, laws, and culture. Thomas P. Hughes, "The Evolution of Large Technological Systems," *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, ed. Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, Anniversary Edition (Cambridge, MA: MIT Press, 2012), 45–76; Thomas P. Hughes, *Networks of Power: Electrification in Western Society, 1880–1930* (1983; repr., Baltimore: Johns Hopkins University Press, 1993).

47. Phillip F. Schewe, *The Grid: A Journey through the Heart of Our Electrified World* (Washington, DC: Joseph Henry Press, 2007).

48. Data drawn from the U.S. Energy Information Administration (EIA), "Summary Statistics for the United States, 2007–2017," *Electric Power Annual 2017*, table 1.2 (Washington, DC: Department of Energy, 2018), https://www.eia.gov/electricity/annual/pdf/epa.pdf; EIA, "Existing Capacity by Energy Source, 2017 (Megawatts)," *Electric Power Annual 2017*, table 4.3; Office of Electricity Delivery and Energy Reliability (OE), *United States Electrical Industry Primer* (Washington, DC: Department of Energy, 2015), 6, 13, https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.

49. EIA, "Total Electric Power Industry Summary Statistics, 2017 and 2016," *Electric Power Annual 2017*, table 1.1.

50. Cost figures for large power transformers taken from the OE, *Large Power Transformers and the U.S. Electric Grid* (Washington, DC: Department of Energy, 2012), 7, https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

51. David Nye, *Electrifying America: Social Meanings of a New Technology, 1880–1940* (Cambridge, MA: MIT Press, 1997).

52. Ibid., ix.

53. Susan Leigh Star foregrounds the relational aspects of infrastructure in her classic overview of infrastructure. Susan Leigh Star, "The Ethnography of Infrastructure," *American Behavioral Scientist* 43, no. 3 (1999): 377–391.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

54. See Collier, Mizes, and Von Schnitzler, "Preface"; Le Dantec and Carl DiSalvo, "Infrastructure and the Formation of Publics in Participatory Design."

55. Rowan v. United States Post Office Department, 397 US 728 (1970).

56. Finn Brunton, *Spam: A Shadow History of the Internet* (Cambridge, MA: MIT Press, 2013), xvi–xvii.

57. Ibid.

58. This synthesis of organizations and culture follows Charles Perrow's work on the history of corporate power in America. Charles Perrow, *Organizing America: Wealth, Power, and the Origins of Corporate Capitalism* (Princeton, NJ: Princeton University Press, 2002).

59. Richard R. John, *Spreading the News: The American Postal System from Franklin to Morse* (Cambridge, MA: Harvard University Press, 1998); Paul Starr, *The Creation of the Media: Political Origins of Modern Communications* (New York: Basic, 2004).

60. Richard F. Hirsh, *Technology and Transformation in the American Electric Utility Industry* (New York: Cambridge University Press, 1989); Hughes, *Networks of Power*.

61. Paul Pierson, *Politics in Time: History, Institutions, and Social Analysis* (Princeton, NJ: Princeton University Press, 2004).

62. Perrow, *Next Catastrophe*; Perrow, *Normal Accidents*; Beck, *Risk Society*; Ulrich Beck, *World at Risk*, trans. Ciaran Cronin (Malden, MA: Polity, 2009).

63. Frank Knight, *Risk, Uncertainty, and Profit* (Chicago: Hart, Schaffner & Marx, 1921; New York: Kelley & Millman, 1957). Citations refer to 1957 edition.

64. Ibid.

65. Ibid.

66. Ibid.

67. Andrew Lakoff, *Unprepared: Global Health in a Time of Emergency* (Oakland: University of California Press, 2017), 16–18.

68. Ibid.

69. Ibid.

70. Perrow, *Normal Accidents*.

71. Ibid.

72. This thread runs through all of Perrow's work. For an explicit focus on power and organizations, see Perrow, *Organizing America*.

73. Beck, *Risk Society*; Beck, *World at Risk*.

74. Ibid.

75. Ibid.

Chapter 1

1. Federal Energy Regulatory Commission (FERC), *The Con Edison Power Failure of July 13 and 14, 1977*, final staff report (Washington, DC: FERC, 1978), 99.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

2. Ibid., 1.

3. Ibid.

4. Ibid.

5. "Blackout: Night of Terror," *Time*, July 25, 1977, 12, 21.

6. Ibid.; "The Blackout," *Washington Post*, July 16, 1977; "The New York Blackout—II Poor Plundering Poor," *Boston Globe*, July 16, 1977; "The Illuminating Blackout," *Hartford Courant*, July 17, 1977.

7. "Blackout: Night of Terror"; Lee Lescaze and Jack Egan, "Power Is Restored in Most Areas; Con Ed is Assailed," *Washington Post*, July 15, 1977.

8. Lescaze and Egan, "Power Is Restored."

9. Ari Goldman, "Still Fun City in Rockaway Peninsula," *New York Times*, July 15, 1977.

10. Ibid.

11. Ibid.

12. Ibid.

13. Ibid.; Tom Goldstein, "Westchester Dark; Long Island's Power Interrupted Briefly," *New York Times*, July 14, 1977.

14. FERC, *Con Edison Power Failure*, 11.

15. On the embeddedness of infrastructures, see Star, "The Ethnography of Infrastructure"; Hughes, *Networks of Power*, 1–17.

16. Perrow, *Normal Accidents*.

17. In this fashion, Perrow's understanding is in line with treatments that consider technologies as containing a set of affordances that make different types of activities more or less likely. See Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006).

18. In this way, normal accident theory is suitable to an "all hazards" approach. See Perrow, *Normal Accidents*; Perrow, *The Next Catastrophe*; Charles Perrow, "Shrink the Targets," *IEEE Spectrum* 43, no. 9 (2006): 46–49.

19. Perrow's theoretical framework is most succinctly presented in Perrow, "Complexity, Coupling, and Catastrophe," chap. 3 in *Normal Accidents*, 62–100. For a discussion of the utility and flexibility of Perrow's conceptual categories, see Karl E. Weick, "Normal Accident Theory as Frame, Link, and Provocation," *Organization and Environment* 17, no. 1 (2004): 27–31.

20. Perrow also discusses the role that indirect information can play. Perrow, *Normal Accidents*, 73.

21. Ibid., 72–84.

22. Ibid.

23. Chris Williams, "Anatomy of OpenSSL's Heartbleed: Just Four Bytes Trigger Horror Bug," *Register*, April 9, 2014, https://www.theregister.co.uk/2014/04/09/heartbleed_explained/.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

24. Perrow, *Normal Accidents*.

25. Ibid., 81–100.

26. Ibid., 93–94.

27. Ibid., 81–100.

28. See also Perrow, *Organizing America*.

29. Perrow, *Normal Accidents*, 88.

30. Work approaching the analysis of infrastructure vulnerability through a focus on network structures fits well within Perrow's lens. See Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: Wiley & Sons, 2006); Sean Gorman, *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection* (Northampton, MA: Edward Elgar, 2005); Albert-László Barabási, *Linked: The New Science of Networks* (New York: Perseus, 2002); Reka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and Attack Tolerance of Complex Networks," *Nature* 406 (2000): 378–382. For a precursor to Perrow's work, see Amory B. Lovins and L. Hunter Lovins, *Brittle Power: Energy Strategy for National Security* (Andover, MA: Brick House, 1982).

31. Perrow, *Normal Accidents*, 78.

32. John, *Spreading the News*.

33. Ibid.

34. David M. Henkin, *The Postal Age: The Emergence of Modern Communications in Nineteenth-Century America* (Chicago: University of Chicago Press, 2007).

35. From the 1790s to the 1820s, the postal system was operated by the General Post Office. In the 1820s, the General Post Office was renamed the Post Office Department (POD). For simplicity, the Post Office Department will be used throughout. James. W. Cortada, *The Digital Hand*, vol. 3, *How Computers Changed the Work of American Public Sector Industries* (New York: Oxford University Press, 2008), 164.

36. Richard B. Kielbowicz, "A History of Mail Classification and Its Underlying Policies and Purposes," prepared for the Postal Rate Commission's Mail Reclassification Proceeding, MC95–1 (Washington, DC, 1995), 8, http://www.prc.gov/Docs/40/40518/PRC-LR-2.pdf.

37. John, *Spreading the News*.

38. Ibid.

39. Ibid.

40. John, *Spreading the News*. See also Richard B. Kielbowicz, *News in the Mail: The Press, Post Office, and Public Information, 1700–1860s* (New York: Greenwood, 1989); Alvin F. Harlow, *Old Post Bags: The Story of the Sending of a Letter in Ancient and Modern Times* (New York: Appleton, 1928), 112–113; George L. Priest, "The History of the Postal Monopoly in the United States," *Journal of Law and Economics* 18, no. 1 (1975): 34–38; Herbert Joyce, *The*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

History of the Post Office: From Its Establishment down to 1836 (London: Bentley & Son, 1893), 7–10; Starr, *The Creation of the Media*, 31–71.

41. John, *Spreading the News*, 59–63; Kielbowicz, *News in the Mail*, 31; Kielbowicz, "History of Mail Classification," 11–12.

42. For example, the Post Office exercised limited discretion concerning classification decisions and determinations concerning whether or not particular articles could be entered into the mail system. See Dorothy G. Fowler, *Unmailable: Congress and the Post Office* (Athens: University of Georgia Press, 1977); Kielbowicz, "History of Mail Classification."

43. John, *Spreading the News*, 206–256; Wayne E. Fuller, *The American Mail: Enlarger of the Common Life* (Chicago: Chicago University Press, 1972), 285–330.

44. The Postal Act of 1792 established penalties for the private carriage of letters that resulted in the injury of Post Office revenue. The Private Express Statutes were amended and recodified by Congress in 1825, 1845, and 1909. See United States Postal Service (USPS), *Report on Universal Service and the Postal Monopoly* (Washington, DC, 2008), http://www.usps.com/postallaw/_pdf/USPSUSOReport.pdf.

45. The postal monopoly changed over time, admitting a number of exceptions at various points. Exemptions included noncommercial carriage, the carriage of prepaid stamped mail by third parties, special messenger services, and letters accompanying cargo. The postal monopoly also did not cover nonletter mail, such as newspapers, or postal service in areas where the Post Office did not operate. USPS, *Report on Universal Service*.

46. President's Commission on Postal Organization, *Towards Postal Excellence: The Report of the President's Commission on Postal Organization* (Washington, DC: Government Printing Office [GPO], 1968), 33–51.

47. Mechanization and automation targeted each of the different stages of mail processing, including culling, separating letters into various sizes and classes; facing, placing the letters in the same direction so they can be read; canceling the postage; and sorting, separating the mail into clusters for the next step of distribution and transportation. USPS, *United States Postal Service: An American History, 1775–2006* (Washington, DC, 2007), 41, https://web.archive.org/web/20090508205717/http://www.usps.com/cpim/ftp/pubs/pub100.pdf; Vern K. Baxter, *Labor and Politics in the U.S. Postal Service* (New York: Plenum Press, 1994), 69–72, 145–150.

48. President's Commission, *Towards Postal Excellence: Commission*, 24, 27.

49. Nicole W. Biggart, "The Post Office as a Business: Ten Years of Postal Reorganization," *Policy Studies Journal* 11, no. 3 (1983): 487; POD, *Postal Progress: An Accounting of Stewardship*, pub. 28 (Washington, DC: GPO, 1968), 7.

50. POD, *Postal Progress*, 5.

51. The Post Office introduced the Sectional Center System in 1963 in conjunction with zip codes as a means of reducing handling costs. Yet the postal system still relied on distributed processing throughout the system, as the continued

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

reliance on manual processing and the absence of mechanization and automation prevented the consolidation of sorting activities into a few central facilities.

52. Clerks during the 1960s could reliably sort letters for roughly 55 different postal facilities at a rate of fewer than 1,000 letters per hour. During the same period, a team of clerks using advanced mechanized multiple-position letter-sorting equipment could sort 28,000 letters per hour into 277 different separations. Baxter, *Labor and Politics*, 70–71.

53. POD, *Annual Report of the Postmaster General, 1969* (Washington, DC: GPO, 1970), 236–241, table 801; President's Commission, *Towards Postal Excellence: Commission*, 16, 170.

54. President's Commission, *Towards Postal Excellence: Commission*, 16, 170; POD, *Annual Report, 1969*, 246, table 804.

55. See Baxter, *Labor and Politics*.

56. President's Commission, *Towards Postal Excellence: Commission*, 161.

57. GAO, *Postal Service: Automation Is Restraining but Not Reducing Costs: GGD-92–58* (Washington, DC, 1992).

58. Baxter, *Labor and Politics*, 70–71.

59. Ibid.

60. The contention that the political structure of postal service slowed the pace and terms of adopting new technologies, detailed below, is central to the observations of the President's Commission on Postal Organization and is echoed in Baxter, *Labor and Politics*. See also the President's Commission, *Towards Postal Excellence: Commission*.

61. Between 1838 and 1968, postal revenues were in the red for all but 17 years. The amount of the deficit fluctuated from year to year, but the President's Commission calculated that as of 1968, the cumulative postal deficit accounted for 15% of total postal costs. During the 1960s, shortfalls were, however, growing; in 1967 the deficit was $1.17 billion, or 19.1% of the total postal budget. President's Commission, *Towards Postal Excellence: Commission*, 22.

62. Ibid., 37.

63. On the connection between the deficit model and disincentives to innovate to reduce costs, see Daniel P. Carpenter, *The Forging of Bureaucratic Autonomy: Reputations, Networks, and Policy Innovation in Executive Agencies, 1862–1928* (Princeton, NJ: Princeton University Press, 2001), 73–94; President's Commission, *Towards Postal Excellence: Commission*, 37.

64. Cortada, *Digital Hand*, 167; see, for example, POD, Office of Research and Engineering, *The Post Office: Challenge to Industry*, publication 48 (Washington, DC: GPO, 1967); POD, *Postal Progress*.

65. On the role of interest group politics and postage, see Jane Kennedy, "United States Postal Rates, 1845–1951" (PhD diss., Columbia University, 1955).

66. Typically, the Post Office would request a new rate increase only once every three to six years. See Arthur D. Little, "A Description of the Postal Service

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Today: Appendix A to the General Contract," Annex contractor's reports, vol. 4, in *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization (Washington, DC: Government Printing Office, 1968), 6–69.

67. Postal rates for first-class letters were established at 3 cents in 1851. Subsequently, they were adjusted as follows: 1883, two cents; 1917, three cents; 1919, two cents; 1932, three cents; 1958, four cents; 1963, five cents; 1968, six cents. In addition to the generally cheap postage afforded second-class mail, second-class postage on in-county publications remained unchanged from 1879 until reorganization. USPS, "Rates for Domestic Letters, 1863–2009" (Washington, DC, 2009), http://www.usps.com/postalhistory/_pdf/DomesticLetterRates1863-2009.pdf; President's Commission, *Towards Postal Excellence: Commission*, 39; Foster Associates, "Rates and Rate-Making," Annex contractor's reports, vol. 2, in *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization (Washington, DC: Government Printing Office, 1968), 2-24.

68. Before the inauguration of the Cost Ascertainment System in 1926, the Post Office did not collect comprehensive cost data on its services. Even after the introduction of the CAS, however, data on cost were disputed and ignored, as Congress fixed rates. See Foster Associates, "Rates and Rate-Making," 2-8-2-13.

69. On this point, see Arthur D. Little, "The U.S. Post Office and Organizational Options for Its Improvement," Annex Contractor's Reports, vol. 1, in *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization (Washington, DC: Government Printing Office, 1968), 109.

70. President's Commission, *Towards Postal Excellence: Commission*, 35–36; Fuller, *American Mail*, 331–341; John T. Tierney, *The U.S. Postal Service: Status and Prospects of a Public Enterprise* (Boston: Auburn, 1988), 9–43; Richard B. Kielbowicz, *Postal Enterprise: Post Office Innovations with Congressional Constraints, 1789–1970*, prepared for the Postal Rate Commission (Seattle, 2000), 63–68, www.prc.gov/tsp/55/enterprise.pdf.

71. Before 1951, funds were made in 58 separate appropriations. Legislation in 1951 simplified the appropriations structure into eight accounts. The Post Office, before 1968, did have limited authority to transfer funds between accounts in amounts that did not exceed more than 2.5% of either donor or acceptor appropriations. Little, "Description of the Postal Service," 6-33-6-34.

72. Ibid., 6-87-6-88.

73. Ibid., 6–30.

74. The disjunction between the time horizons of elected officials and the requirements of long-term planning are explored clearly by Pierson, *Politics in Time*.

75. By the late 1960s, 87.5% of postal workers were represented by 1 of 12 craft unions. The largest two unions, the National Association of Letter Carriers and the United Federation of Postal Clerks, represented well over half of all postal employees. President's Commission, *Towards Postal Excellence: Commission*, 18–19.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

76. They did this not only by lobbying Congress to limit the amount of money appropriated for investment in new technology but also by refusing to fully cooperate with some equipment field tests. See Baxter, *Labor and Politics*, 73–74.

77. Figure calculated from data in Little, "Description of the Postal Service," 4–23, table 4.1.11.

78. Calculated from data in ibid., 4-20-4-23, table 4.1.11; POD, *Annual Report, 1969*, 246, table 804.

79. Little, "Description of the Postal Service," 4–20.

80. President's Commission, *Towards Postal Excellence: Commission*, 27.

81. See "Frequently Asked Questions," Smithsonian National Postal Museum, accessed September 20, 2017, http://postalmuseum.si.edu/about/frequently-asked-questions/index.html#history10.

82. Perrow highlights in passing the postal system as an example of a loosely coupled system, though he does not provide an analysis of the network. Perrow, *Normal Accidents*, 97–99.

83. Theodore E. Keeler, *Railroads, Freight, and Public Policy* (Washington, DC: Brookings Institution, 1983), 19–20; Ari Hoogenboom and Olive Hoogenboom, *A History of the ICC: From Panacea to Palliative* (New York: Norton, 1976), 7.

84. Railroads provided many obvious benefits over other modes of transportation. Unlike other forms of overland transportation, such as canals, the railroads were quicker, cheaper, and far more reliable—particularly in difficult weather conditions. Alfred D. Chandler Jr., *The Visible Hand: The Managerial Revolution in American Business* (1977; repr., Cambridge, MA: Harvard University Press, 1993), 86.

85. Despite support for subsidy, these same groups rarely called for public ownership of the railroads during the early period of development. Only a small number of railroads in the United States were ever operated as public enterprises, and by 1850, with few exceptions, these were transferred to private hands. Ibid., 82; Frederick C. Clark, *State Railroad Commissions, and How They May Be Made Effective* (Baltimore: Guggenheimer and Weil, 1891), 12–14.

86. During the period before 1861, 30% of all funding for railroad building came from the state. The states spent an estimated $350 million on railroads and canals before 1873. Gabriel Kolko, *Railroads and Regulation, 1877–1916* (Princeton, NJ: Princeton University Press, 1965), 15; Horwitz, *Irony of Regulatory Reform*, 54.

87. Eminent domain law allowed states to annex private land and provide it at a discounted price for the purpose of supporting the growth of railroads. The granting of rights-of-way plainly reduced the costs of constructing railroads and made them more feasible. Horwitz, *Irony of Regulatory Reform*, 49–54; Keeler, *Railroads, Freight, and Public Policy*, 20; Chandler, *Visible Hand*, 82; Richard Stone, *The Interstate Commerce Commission and the Railroad Industry: A History of Regulatory Policy* (New York: Praeger, 1991), 2–3.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

88. Chandler, *Visible Hand*, 83.

89. Ibid.; Horwitz, *Irony of Regulatory Reform*, 58.

90. Often, railroads set local rates above through rates in an effort to capture long-haul traffic. This long/short divide disadvantaged farm producers and merchants situated on interior lines, who were effectively bypassed in favor of those situated at the ends of the lines. Hoogenboom and Hoogenboom, *History of the ICC*, 4–5.

91. Undisclosed rebates and drawbacks (rebates on competitor's freight) were used by the railroads to capture certain large industrial shippers and drew immense disapproval from competitors that were denied such benefits. Famously, Standard Oil was a beneficiary of such practices. Ibid., 5.

92. For example, 1,300 farmers spread across eight different Wisconsin counties mortgaged their farms to raise $1.5 million to attract rail service. Stone, *Interstate Commerce Commission*, 2–3; Hoogenboom and Hoogenboom, *History of the ICC*, 6–7.

93. Stone, *Interstate Commerce Commission*, 4; Horwitz, *Irony of Regulatory Reform*, 58; Wesley R. Kriebel and C. Phillip Baumel, "Issues in Freight Transportation Regulation," *American Journal of Agricultural Economics* 61, no. 5 (1979): 1003–1009; Lee Benson, *Merchants, Farmers, and Railroads: Railroad Regulation and New York Politics* (Cambridge, MA: Harvard University Press, 1955); Ida M. Tarbell, *The History of the Standard Oil Company* (New York: McClure, Philips, 1904).

94. Hoogenboom and Hoogenboom, *History of the ICC*, 5.

95. Under conditions of high fixed costs, increased volume does not dramatically alter cost. Hence, where competition exists, the inclination to slash rates to attract greater volume is acute. One estimate stated that during the 1880s as much as two-thirds of rail costs did not vary with volume carried. Chandler, *Visible Hand*, 134; Hoogenboom and Hoogenboom, *History of the ICC*, 2–3.

96. These practices were self-defeating and led to cycles of boom and bust. Freight revenue per ton-mile declined between 1870 and 1900 (just before ICC regulation became effective in maintaining stability) from $1.88 in 1870 to $1.22 in 1880, $0.94 in 1890, and, finally, $0.73 in 1900. Large customers on competitive lines extracted rebates of up to 50% of the published rate as railroads scrambled to maintain traffic levels. During the rate war of 1876 and 1877, eastbound freight rates fell from $1.00 to $0.15 per 100 lbs., while freight rates heading west fell from $0.75 to $0.25. Keeler, *Railroads, Freight, and Public Policy*, 21–22; Hoogenboom and Hoogenboom, *History of the ICC*, 2–3; Kolko, *Railroads and Regulation*, 7–12; Chandler, *Visible Hand*, 134–143; Horwitz, *Irony of Regulatory Reform*, 60–61; George W. Hilton, "The Consistency of the Interstate Commerce Act," *Journal of Law and Economics* 9 (1966): 90.

97. The first pools were formed as early as the 1850s. The major pools were created during the 1870s, first as informal agreements between regional competitors and then as formal administrative federations containing executive, legislative,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and judicial branches. Hoogenboom and Hoogenboom, *History of the ICC*, 4–5; Kolko, *Railroads and Regulation*, 8–9; Chandler, *Visible Hand*, 135.

98. Of the eight pools in operation in 1879, all but one rapidly failed. Chandler argues that consolidation and expansion helped buffer the ruinous effects of competition and, as a result, helped stabilize the industry to a greater degree than federal regulation. Yet, as Chandler later notes, these efforts did not eliminate rebates or drawbacks, two key elements of ruinous competition. Indeed, ruinous competition continued after the railroads pursued the creation of integrated systems. *Visible Hand*, 142–187. See also Kolko, *Railroads and Regulation*, 7–19, 64–101.

99. The first state commission was established in 1832 in Connecticut, though commissions remained irregular until the 1860s. Between 1860 and 1887, 20 state commissions were in operation; in New England, all states, with the exception of New Hampshire, had state commissions, while the Grange successfully pushed for strong state commissions in the Midwest. Generally, state commissions attempted to ensure that railroads operated as common carriers and did not refuse service, charged reasonable and nondiscriminatory rates, and did not discontinue or abandon service without the consent of those served. These provisions were, however, often self-enforcing and, as result, translated into little practical control. The majority of state commissions were weak; of 20 state commissions, only 8 had the power to set mandatory rates. The remaining commissions acted as advisory boards, with little power of enforcement. Benson, *Merchants, Farmers, and Railroads*, 1–2; Hoogenboom and Hoogenboom, *History of the ICC*, 7; Kolko, *Railroads and Regulation*, 16.

100. The case considered the status of state controls over the economy and, specifically, the granger laws. The case focused on grain elevators but was directly linked to the railroad issue. As the court opinion clarifies: "Property does become clothed with a public interest when used in a manner to make it of public consequence, and affect the community at large. When, therefore, one devotes his property to a use in which the public has an interest, he, in effect, grants to the public an interest in that use, and must submit to be controlled by the public for the common good, to the extent of the interest he has thus created." The common-law principle of common callings, or, as it became known within the realm of transportation, common carriers, was applied to a wide swath of activities, including canals, turnpikes, millers, inns, and railroads. Munn v. Illinois, 94 U.S. 113, 116 (1876); Horwitz, *Irony of Regulatory Reform*, 49.

101. *Munn v. Illinois*, 94 U.S. at 132.

102. Horwitz, *Irony of Regulatory Reform*, 58; Hoogenboom and Hoogenboom, *History of the ICC*, 8; C. Gregory Bereskin, "Regulation, Deregulation, and Reregulation in the Surface Transportation Industry," in *Transportation in the New Millennium: State of the Art and Future Directions, Perspectives from Transportation Research Board Standing Committees* (Washington, DC: Transportation Research Board, 2000), http://onlinepubs.trb.org/onlinepubs/millennium/00097.pdf.

103. Wabash, St. Louis & Pacific Railway Company v. Illinois, 118 U.S. 557 (1886); Hoogenboom and Hoogenboom, *History of the ICC*, 8; Keeler, *Railroads, Freight, and Public Policy*, 22; Horwitz, *Irony of Regulatory Reform*, 58–61.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

104. Keeler, *Railroads, Freight, and Public Policy*, 22; Hoogenboom and Hoogenboom, *History of the ICC*, 18; Kolko, *Railroads and Regulation*, 44.

105. Stone, *Interstate Commerce Commission*, 5; Horwitz, *Irony of Regulatory Reform*, 63.

106. Keeler, *Railroads, Freight, and Public Policy*, 23.

107. Ibid., 22.

108. Hoogenboom and Hoogenboom, *History of the ICC*, 17–18.

109. Ibid., 118; Kolko, *Railroads and Regulation*, 45–63.

110. Kolko, *Railroads and Regulation*, 45–63.

111. After some initial success in enacting rail regulations, a series of court decisions in the 1890s circumscribed the power of the commission. In 1889, during the first appeal of an ICC decision, the presiding Federal Circuit Court ruling insisted on rehearing and examining evidence previously submitted. As a result, the courts routinely considered new evidence and reevaluated evidence already presented to the ICC during the appeals process. This practice undercut the authority of the commission and gave the courts tight control over the regulatory process. During the 1890s, the Supreme Court further reduced the power and effectiveness of the ICC. In *Smyth v. Ames* (1898) (also known as *Maximum Freight Rate*), the court stripped the ICC of the power to set rates, while in *U.S. v. Trans-Missouri* (1897) the court argued that cartel agreements and joint rates, which the ICC had moved to adopt and support, violated the Sherman Antitrust Act. Horwitz, *Irony of Regulatory Reform*, 11; Stone, *Interstate Commerce Commission*, 7–8; Hoogenboom and Hoogenboom, *History of the ICC*, 30–31; Kolko, *Railroads and Regulation*, 71–83; Smyth v. Ames, 169 US 466 (1898); U.S. v. Trans-Missouri 166 US 290 (1897).

112. These were the Elkins Act (1903), the Hepburn Act (1906), and the Mann-Elkins Act of 1910. The Elkins Act made the published rate the legal rate and made deviations, such as rebates, punishable by law. The act also allowed for joint or collective rate making by the railroads. The Hepburn Act gave the ICC the power to replace existing rates and made ICC decisions binding, shifting power away from the courts and back to the ICC. It also provided the ICC with the power to appoint examiners and agents to inspect railroad accounts. Finally, the Mann-Elkins Act gave the ICC the power to suspend rates and determine if circumstances between routes were substantially different enough to warrant pricing differences. Together, the acts provided the ICC with powers that the courts had previously neutered. Keeler, *Railroads, Freight, and Public Policy*, 23; Stone, *Interstate Commerce Commission*, 10–12; Kolko, *Railroads and Regulation*, 58–61; Hoogenboom and Hoogenboom, *History of the ICC*, 60–61.

113. Performance under regulation increased: between 1888 and 1910, the percentage of railroad stocks paying dividends rose from 39% to 67%; during the same period, the average rate of dividends paid increased from 2.1% to 5%. Kolko, *Railroads and Regulation*, 232.

114. Although pooling was formally prohibited by the ICC, from its very beginning it achieved the desired end: the elimination of rate competition.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

In drawing regulations the ICC allowed, informally at first and then legally, collective rate making through rate associations and eventually set maximum and minimum rate thresholds. Eventually, the Transportation Act of 1920 legalized pools, subject to ICC approval. Hoogenboom and Hoogenboom, *History of the ICC*, 18–29, 60–61, 109; Kolko, *Railroads and Regulation*, 58–63, 100.

115. Kolko, *Railroads and Regulation*, 58–63, 100; Keeler, *Railroads, Freight, and Public Policy*, 25–46.

116. Federal regulations also provided the railroads with a single set of predictable standards. One of the key concerns of rail interests before the enactment of federal regulations centered on the unpredictability of regulations at the state level. Federal regulations eliminated this problem and allowed the railroads to engage in long-term planning with some confidence. Kolko, *Railroads and Regulation*, 116–117, 232; Horwitz, *Irony of Regulatory Reform*, 34; Keeler, *Railroads, Freight, and Public Policy*, 23.

117. This principle was consistently put into practice by the ICC and appeared as early as 1890. The 1914 ICC ruling on a proposed general rate increase, in what is known as the 5 Percent Case, formalized this policy. The 1920 Transportation Act fixed the rate of return at 6%. Stone, *Interstate Commerce Commission*, 21; Kolko, *Railroads and Regulation*, 54, 210–217.

118. The predictability of published rates also allowed shippers to better forecast their costs and plan accordingly. Stone, *Interstate Commerce Commission*, 11; Hoogenboom and Hoogenboom, *History of the ICC*, 3, 42–45; Kolko, *Railroads and Regulation*, 93–96.

119. Keeler, *Railroads, Freight, and Public Policy*, 22–23; Horwitz, *Irony of Regulatory Reform*, 60–63.

120. One of the key aims of the Transportation Act of 1920 was to introduce a plan to consolidate the railroad system into a more efficient network. Such a plan was commissioned but ultimately ignored. Keeler, *Railroads, Freight, and Public Policy*, 26.

121. Jean-Paul Rodrigue, Claude Comtois, and Brian Slack, *The Geography of Transport Systems* (New York: Routledge, 2009), http://people.hofstra.edu/geotrans/index.html.

122. Redundant track included both small branch lines unsupported by traffic and duplicate or parallel lines connecting two points. Hilton, "Interstate Commerce Act," 92–93.

123. Rodrigue, Comtois, and Slack, *Geography of Transport Systems*.

124. The redundancy and excess capacity of the railroad system was not, then, simply a by-product of the growth of other modes of transportation (such as air and truck). Rather, it was established during the 19th-century growth of the network. The development of competing modes merely reinforced these qualities. Richard C. Levin, "Regulation, Barriers to Exit, and the Investment Behavior of Railroads," in *Studies of Economic Regulation*, ed. Gary Fromm (Cambridge, MA: MIT Press, 1981), 184.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

125. Keeler, *Railroads, Freight, and Public Policy*, 26, 42; William R. Dougan, "Railway Abandonments, Cross-Subsidies, and the Theory of Regulation," *Public Choice* 44, no. 2 (1984): 300–301.

126. Keeler, *Railroads, Freight, and Public Policy*, 21–39.

127. In the decade before deregulation, only 1% of total track was put up for abandonment. Of proposed abandonments, nearly all, 97.5%, were approved by the ICC. Levin, "Regulation," 216–217; Dougan, "Railway Abandonments," 302.

128. Keeler, *Railroads, Freight, and Public Policy*; Dougan, "Railway Abandonments," 302; Levin, "Regulation," 182; Rodrigue, Comtois, and Slack, *Geography of Transport Systems*.

129. Keeler, *Railroads, Freight, and Public Policy*, 42.

130. For a discussion of the history of DT&I conditions, see Darius W. Gaskins, "Regulation of Freight Railroads in the Modern Era: 1970–2010," *Review of Network Economics* 7, no. 4 (2008), doi:10.2202/1446–9022.1162; Detroit, Toledo, and Ironton v. ICC, 725 F.2d 47 (1984).

131. Value-of-service pricing encouraged, by design, the widest possible utilization of the rail network and specifically encouraged rural farmers to ship via rail. In this way it also supported the continuation of an expansive network; whereas cost-of-service pricing would have discouraged the use of costly rural services, the adoption of value-of-service pricing encouraged wide use of the network. Stone, *Interstate Commerce Commission*, 13; Keeler, *Railroads, Freight, and Public Policy*, 14; Ann F. Friedlaender and Richard H. Spady, *Freight Transport Regulation: Equity, Efficiency, and Competition in the Rail and Trucking Industries* (Cambridge, MA: MIT Press, 1981), 1–3.

132. Ann F. Friedlaender, *The Dilemma of Freight Rail Transportation* (Washington, DC: Brookings Institution, 1969), 101.

133. Historically, states and local governments also provided funding for the development of roads.

134. Friedlaender, *Dilemma*, 1–27, 65–127; John Meyer et al., *The Economics of Competition in the Transportation Industries*, Harvard Economic Studies (Cambridge, MA: Harvard University Press, 1959); Keeler, *Railroads, Freight, and Public Policy*, 8–29.

135. GAO, *Railroad Regulation: Economic and Financial Impact of Staggers Rail Act of 1980*, GAO/RCED-90–80 (Washington, DC, 1990), 53.

136. United States Census Bureau, *Commodity Transportation Survey, Economic Census* (Washington, DC: GPO, 1963, 1967, 1972, 1977).

137. Transportation Research Board, *Cooperative Research for Hazardous Materials Training: Defining the Need, Converging on Solutions—Special Report 283* (Washington, DC: National Academies Press, 2005), 19, doi:10.17226/11198. For detailed information, see also U.S. Department of Transportation, *Commodity Flow Survey, Economic Census: Transportation* (Washington, DC, 1993–2016), http://www.bts.gov/publications/commodity_flow_survey/.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

138. For a detailed discussion, see D. F. Brown, W. E. Dunn, and A. J. Policastro, *A National Risk Assessment for Selected Hazardous Materials in Transportation* (Argonne, IL: Argonne National Laboratory, 2000).

139. A *natural monopoly* is an industry with economies of scale in which average cost decreases as the size of the producing firm increases. Under these conditions, it is most beneficial to have one firm operating. See Alfred Kahn, "The Role and Definition of Competition: Natural Monopoly," in *The Economics of Regulation: Principles and Institutions*, vol. 2, *Institutional Issues* (New York: Wiley and Sons, 1971), 113–171.

140. Mark Granovetter and Patrick McGuire, "The Making of an Industry," in *Laws of the Markets*, ed. Michel Callon (New York: Blackwell, 1998), 147–73. See also Hughes, *Networks of Power*, 216–229; Richard F. Hirsh, *Power Loss: The Origins of Deregulation and Restructuring in the American Electric Utility System* (Cambridge, MA: MIT Press, 1999), 23–26; Douglas D. Anderson, *Regulatory Politics and Electric Utilities: A Case Study in Political Economy* (Boston: Augurn, 1981), 33–56.

141. Sharon Beder, *Power Play: The Fight to Control the World's Electricity* (New York: New Press, 2003), 30.

142. Granovetter and McGuire, "Making of an Industry"; Richard F. Hirsh, "Emergence of Electrical Utilities in America," *Powering the Past: A Look Back*, Smithsonian Institute, last modified September 2002, http://americanhistory.si.edu/powering/past/h1main.htm.

143. John F. Wasik, *The Merchant of Power: Sam Insull, Thomas Edison, and the Creation of the Modern Metropolis* (New York: Palgrave Macmillan, 2006), 3, 170, 203.

144. Ibid.

145. Insull was an early booster of the steam turbine as a replacement for the reciprocating steam engine. Steam turbines utilized roughly one-tenth the space of reciprocating steam engines and, eventually, were able to generate far greater amounts of power. Ibid.

146. This model of electricity provision, which Edison in effect inaugurated with the Pearl Street Station, is often described as centralized, as it pairs generation and a network of users. However, it is important to note that the degree of centralization was qualified and limited. As will be discussed below, control was organized at the level of individual power systems and the electric power grid, in aggregate, comprised a web of functionally discrete and autonomous linked systems. Note: transmission lines are high-voltage lines running from generating plants to substations; distribution lines are lower-voltage lines that connect directly to end users.

147. Insull divided customers into 11 different classes of consumers in order to analyze the diversity of demand. He particularly prized ice manufacturers because their demand was at its lowest on cold days when demand from other customers was at its peak. Hughes, *Networks of Power*, 217–218.

148. These ideas were not Insull's alone. British engineer John Hopkinson and electricity manager Arthur Wright pioneered and outlined the importance of the

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

concepts of *load factor*, the ratio between average and peak demand, and the diversity of demand for electricity that Insull adopted. Hirsh, *Technology and Transformation*, 17–18; Hirsh, "Emergence"; Hughes, *Networks of Power*, 216–219.

149. Indeed, until 1915 the majority of consumers in the U.S. relied on isolated systems for electric power. Granovetter and McGuire, "Making of an Industry."

150. Chicago, for example, issued 20 nonexclusive, competitive franchises between 1882 and 1905. Hirsh, *Power Loss*, 14.

151. Ibid., 15; Beder, *Power Play*, 24.

152. Hirsh, *Power Loss*, 13–14.

153. Hirsh, *Power Loss*, 13; Wasik, *Merchant of Power*, 79–81.

154. Beder, *Power Play*, 27; Hughes, *Networks of Power*, 207.

155. Forrest McDonald, "Samuel Insull and the Movement for State Utility Regulatory Commissions," *Business History Review* 32, no. 3 (1958): 241–254; Granovetter and McGuire, "Making of an Industry"; Hirsh, *Power Loss*, 21–23.

156. Hirsh, "Emergence"; Hirsh, *Power Loss*, 19–23; Anderson, *Regulatory Politics*, 48.

157. Generally, Progressives sought across spheres of the economy, not only in electric power, to harness the seeming inherent advantages afforded by large corporate operations with the tempering influence of state oversight. See Hirsh, *Power Loss*, 23; Arthur Schlesinger Jr., *Crisis of the Old Order, 1919–1933* (Boston: Houghton Mifflin, 1957).

158. Beder, *Power Play*, 27–30; Hughes, *Networks of Power*, 207; McDonald, "Samuel Insull," 251; Anderson, *Regulatory Politics*, 4–16.

159. State regulatory bodies controlled entry through the granting of franchises. James E. Meeks, "Concentration in the Electric Power Industry: The Impact of Antitrust Policy," *Columbia Law Review* 72, no. 1 (1972): 95–96.

160. Hirsh, "Emergence"; Beder, *Power Play*, 28–30; Granovetter and McGuire, "Making of an Industry."

161. Hirsh, "Emergence."

162. Hirsh, "Emergence"; Beder, *Power Play*, 28–30; Granovetter and McGuire, "Making of an Industry."

163. Hirsh, *Power Loss*, 15–31.

164. Ibid., 26–27; Beder, *Power Play*, 28–29; Anderson, *Regulatory Politics*, 61–88.

165. Hughes, *Networks of Power*, 325.

166. Hughes, *Networks of Power*, 292.

167. The war drove demand for electricity and stressed the capacity of providers, particularly in areas undertaking the production of munitions and shipbuilding. In 1917, army engineers working under the newly formed War Industries Board conducted a survey of U.S. generating capacity in order to determine if the electric power facilities were sufficient to support mobilization.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Even though new, fast-tracked construction projects would have increased generating capacity by 10% in two years, the study forecast dire shortfalls that could have crippled the war effort. Leonard DeGraaf, "Corporate Liberalism and Electric Power System Planning in the 1920s," *Business History Review* 64, no. 1 (1990): 15; Thomas P. Hughes, "Technology and Public Policy: The Failure of Giant Power," *Proceedings of the IEEE* 64, no. 9 (1976): 1363; Hughes, *Networks of Power*, 289–292.

168. Hughes, *Networks of Power*, 292; Hughes, "Technology and Public Policy," 1361–1372; DeGraaf, "Corporate Liberalism," 1–31.

169. Hughes, *Networks of Power*, 289–292.

170. The voltage of transmission lines doubled every 10 years during the early 1900s. In 1900, 50,000 V lines were commercially available; in 1910, 110,000 V lines were available; and in 1920, 220,000 V were in use. Hughes, "Technology and Public Policy," 1362.

171. Hughes, *Networks of Power*, 292; Hughes, "Technology and Public Policy," 1361–1372; DeGraaf, "Corporate Liberalism," 1–31.

172. Julie A. Cohen, *The Grid: Biography of an American Technology* (Cambridge, MA: MIT Press, 2017), 126.

173. On the differences among the plans, see DeGraaf, "Corporate Liberalism."

174. Super Power sought to integrate electric power systems stretching from Boston to Washington, DC, into a single system boosted by additional large plants and transmission lines under the control of a new advisory board, the North America Super Power Board, which would assume the role of coordinating the distribution of power across the newly interconnected system of utilities. Giant Power, as envisioned, was a more radical public intervention. It called for a new Giant Power Board and the creation of new plants situated at mine mouths in Pennsylvania that could export power to load centers throughout the state and, eventually, to New York and New Jersey as well, across high-voltage transmission lines. Under this system, the state would reserve the right to take over private facilities in 50 years, and a stricter policy for setting rates that was not as hospitable to utilities would be implemented. Ibid., 1–12; Hughes, *Networks of Power*, 296–313.

175. Initially, private utilities voiced some support for Super Power when it was first discussed in 1919. Quickly, however, as capital markets loosened and holding companies began having success at integrating operations outside of government control, industry turned against plans for Super Power. DeGraaf, "Corporate Liberalism," 11.

176. Hughes, *Networks of Power*, 308.

177. Hirsh, "Emergence"; U.S. Energy Information Administration (EIA), *Public Utility Holding Company Act of 1935: 1935–1992* (Washington, DC: Department of Energy, 1993), 5–6, https://www.eia.gov/electricity/archive/0563.pdf; Benjamin Graham and David Dodd, *Security Analysis: The Classic 1940 Edition*, 2nd ed. (New York: McGraw-Hill, 2002).

178. Between 1922 and 1927, the number of holding companies increased from 102 to 180, while the number of operating companies actually declined, from

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

roughly 6,000 to 4,000. In the following years, the trend toward consolidation continued as the ownership of more than half of all private utility companies changed hands. From 1927 to 1930, there were an astounding 2,500 changes of ownership, the majority involving holding companies gaining control over independent operators. Hirsh, "Emergence"; EIA, *Public Utility*, 5–6.

179. Holding companies not only served as tools for speculation and the overvaluation of operating companies. They also provided some legitimate benefits. They attracted investment to the capital-intensive industry and allowed the pooling of technical and managerial resources between previously failing smaller utilities and larger units. Hirsh, *Technology and Transformation*, 23–24; William Emmons III, "Franklin D. Roosevelt, Electric Utilities, and the Power of Competition," *Journal of Economic History* 53, no. 4 (1993): 883.

180. Three holding companies controlled nearly half the electricity in the country. "Section 11(b) of the Holding Company Act: Fifteen Years in Retrospect," *Yale Law Journal* 59, no. 6 (1950): 1088; Emmons, "Franklin D. Roosevelt," 883.

181. "Section 11(b)," 1111; DeGraaf, "Corporate Liberalism." For a larger discussion of the rise and breadth of holding companies, see Hughes, *Networks of Power*, 363–403.

182. Beder, *Power Play*, 62; Hughes, *Networks of Power*, 400–401.

183. Hughes, *Networks of Power*, 400–401; Hughes, "Technology and Public Policy," 1368.

184. Hughes, "Technology and Public Policy," 1363, 1368.

185. Emmons, "Franklin D. Roosevelt," 883; Hirsh, "Emergence"; "Section 11(b)," 1099.

186. Though none quite as spectacularly as Insull's Middle West Utilities Company. In 1929 shares of Insull's company traded at $57 but were worth only $0.25 in 1932 before it declared what was at the time the largest bankruptcy in history. The damage was stark: 100,000 stockholders lost what would today be roughly $4 billion, including company employees who had been exhorted to invest in the company. The Middle West Utilities Company was unique only in the size of the failure, as the Great Depression drove holding companies, and the larger economy, to ruin. Beder, *Power Play*, 64; Emmons, "Franklin D. Roosevelt," 883–885; EIA, "Public Utility," 1–8; Hirsh, *Power Loss*, 40; "Section 11(b)," 1089.

187. Wasik, *Merchant of Power*, 200.

188. Ibid., 201.

189. Quoted in Beder, *Power Play*, 65; Hirsh, "Emergence." See also EIA, "Public Utility," 1–8; Emmons, "Franklin D. Roosevelt," 883–885.

190. Roosevelt attacked the utility problem through three directions: (1) The PUHCA sought to break up holding companies and return them to effective state control; (2) the Tennessee Valley Authority attempted to spur regional economic development and lower electricity prices through the introduction of regional competition via the new public project; (3) the Rural Electric Administration made available loans to assist rural cooperatives in setting up their

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

own power systems. Though each of these initiatives was important, I focus on PUHCA, as it most directly affected the architecture of electric power networks. Emmons, "Franklin D. Roosevelt," 885–886. On the run up to the PUHCA, see also Hughes, *Networks of Power*, 392–393.

191. EIA, "Public Utility," 1; Emmons, "Franklin D. Roosevelt," 883–885.

192. "Section 11(b)," 1094.

193. Ibid., 1094–1104; Hirsh, "Emergence."

194. Multiple systems could be retained if a system (1) could not otherwise be operated without a substantial economic burden, (2) resided in the same or adjoining state, and (3) would not impair the advantage of local management. In practice, the SEC developed a strict interpretation of the new law and required that systems be fully integrated and serve a single area (known as the *single-area interpretation*). "Section 11(b)," 1100–1104.

195. The number of holding companies registered with the SEC dropped to less than 20, while over 750 systems with assets valued at over $7 billion were divested from various holding companies. For a thorough discussion of section 11(b) and its scope, purpose, and eventual interpretation, see "Section 11(b)."

196. Ibid., 1104.

197. Hughes, *Networks of Power*, 401.

198. Barney Capehart, ed., *Encyclopedia of Energy Engineering and Technology* (Boca Raton: CRC Press, 2007), 392; "Section 11(b)," 1111.

199. Meeks, "Concentration," 67–69.

200. Cohen, *Grid*.

201. Hughes, *Networks of Power*, 372–374; Theodore J. Nagel, "Operation of a Major Electric Utility Today," *Science* 201, no. 4360 (1978): 985; F. D. Boardman, "Future Developments in the Control of Power Systems," *Philosophical Transactions of the Royal Society of London, Series A, Mathematical and Physical Sciences* 275, no. 1248 (1973): 244; James M. Griffin and Steven L. Puller, "Introduction: A Primer on Electricity and the Economics of Deregulation," in *Electricity Deregulation: Choices and Challenges* (Chicago: University of Chicago Press, 2005), 5.

202. Cohen, *Grid*, 51.

203. As Hughes notes, the central dispatcher had to be something of a historian, understanding patterns of use for the area under control. As early as 1910, central dispatch regularly had access to compiled records displaying hourly system output going back several years that could be matched against demand. *Networks of Power*, 215. For an overview of the use of real-time technologies in electrical power, see Nathan Cohn, "Recollections of the Evolution of Realtime Control Applications to Power Systems," *Automation* 20, no. 2 (1984): 145–162; Nagel, "Operating." For a detailed technical discussion of the history of control technology as it relates to electrical power and beyond, see Stuart Bennett, *A History of Control Engineering, 1800–1930* (New York: Institution of Electrical Engineers, 1979); Stuart Bennett, *A History of Control Engineering, 1930–1955* (London: Institution of Electrical Engineers, 1993).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

204. Hirsh, *Technology and Transformation*, 80–82; Anderson, *Regulatory Politics*; GAO, *Changes in Electricity-Related R&D*, GAO/RCED-96–203 (Washington, DC, 1996), 3.

205. The normative case suggesting that firms under rate-of-return regulation seek investment in capital-intensive projects as a means of expanding profit is dealt with in the classic work by Harvey Averch and Leland L. Johnson, "Behavior of the Firm under Regulatory Constraint," *American Economic Review* 52, no. 5 (1962): 1052–1069. The general phenomena, as a result, are known as the *Averch-Johnson effect* in the economics literature. See also E. David Emery, "Regulated Utilities and Equipment Manufacturers' Conspiracies in the Electric Power Industry," *Bell Journal of Economics and Management Science* 4, no. 1 (1973): 322–337.

206. State regulatory commissions did not have the staff to provide such detailed oversight. Nor was there a real call to do so until the upheavals of the 1970s and the advent of regulatory activism, which will be discussed in the next chapter. This gap, between shifting costs and unadjusted, stable rates, is known as regulatory lag. Hirsh, *Technology and Transformation*, 112–113, 150–152; Anderson, *Regulatory Politics*, 71.

207. Nathan Cohn et al., "On-Line Computer Applications in the Electric Power Industry," *Proceedings of the IEEE* 58, no. 1 (1970): 78.

208. The replacement of manual controls with automated, computerized controls reduced but did not eliminate the hand of the operator. In addition to the programming and maintenance, even closed-loop automated power systems required a degree of operator oversight and contained interfaces to this end. Nagel, "Operating," 988.

209. Hirsh, *Technology and Transformation*, 84; Cohen, *Grid*.

210. This is not to say that such technologies did not improve utility performance or that utility managers did not see their adoption as a good faith effort to improve operation. Rather, the structure of incentives as designed under rate-of-return regulation simply made adoption more attractive regardless.

211. Vannevar Bush suggested that there were essentially three different ways to study the stability of power systems: direct experience, test of laboratory models, and mathematical analysis. Bush turned toward the latter two options; the actual systems were too new, expensive, and complex to allow direct experimentation and testing. David A. Mindell, *Between Human and Machine: Feedback, Control, and Computing before Cybernetics* (Baltimore: Johns Hopkins University Press, 2002), 146; Larry Owens, "Vannevar Bush and the Differential Analyzer: The Text and Context of an Early Computer," *Technology and Culture* 27, no. 1 (1986): 66–67.

212. GE provided funding, equipment, and facilities and shared research. The linkages between MIT and GE extended to an innovative cooperative master's program that combined study and periods of work at GE's Lynn plant, which graduated its first class in 1922. Hughes, *Networks of Power*, 376–377; Mindell, *Between Human and Machine*, 152–158; Fredrick E. Terman, "A Brief History of Electrical Engineering Education," *Proceedings of the IEEE* 86, no. 8

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

(1998): 1796–1797, classic paper, reprinted from *Proceedings of the IEEE* 64, no. 9 (1976): 1399–1406; Aristotle Tympas, "Perpetually Laborious: Computing Electric Power Transmission before the Electric Computer," *International Review of Social History* 48 (2003): 73–95.

213. The study of transients was central to the work Bush and the Electrical Engineering Department of MIT conducted during the 1920s and early 1930s. The network analyzer used small transformers as generators and motors, artificial lines, and a plugboard from a telephone exchange to allow reconfiguration. The network analyzer reproduced a 200 mi. system within 50 ft.^{2} and differed from other earlier models and AC and DC calculating boards in that it was programmable: it could be reconfigured to represent and model different systems. The differential analyzer was the latest in a line of mechanical calculating machines that included the earlier intergraph. For an overview of the creation of the network analyzer and the differential analyzer, see Mindell, *Between Human and Machine*, 143–158; Owens, "Vannevar Bush," 63–95; Hughes, *Networks of Power*, 376–377; Aristotle Tympas, "From Digital to Analog and Back: The Ideology of Intelligent Machines in the History of the Electric Analyzer, 1870s–1960s," *IEEE Annals of the History of Computing* 18, no. 4 (1996): 42–48.

214. Mindell, *Between Human and Machine*, 152–153, 157–158; Tympas, "From Digital to Analog," 45.

215. For a detailed overview of Westinghouse's R&D of computational and computing equipment, see William Aspray, "Edwin L. Harder and the Anacom: Analog Computing at Westinghouse," *IEEE Annals of the History of Computing* 15, no. 2 (1993): 35–52.

216. Hughes, *Networks of Power*, 377; Thomas Haigh, Mark Priestley, and Crispin Rope, *ENIAC in Action: Making and Remaking the Modern Computer* (Cambridge, MA: MIT Press, 2018), 7.

217. Gene Smith, "Computer to Get New Power Role," *New York Times*, July 6, 1958, F1.

218. For contemporary news accounts, see Smith, "Computer to Get New Power Role"; "Daystrom to Build System for Utility," *New York Times*, March 12, 1959, New York edition, 40; Gene Smith, "Automation Due in Power Plants," *New York Times*, February 5, 1961, F1; "Computer Industry Chalks Up a Big Day," *New York Times*, April 4, 1963, New York edition, 67; Gene Smith, "Power Industry Adds Computers," *New York Times*, October 8, 1964, New York edition, 63.

219. Robert H. Miller, *Power System Operation* (New York: McGraw-Hill, 1983), 47; Jerry Russell, "Brief History of SCADA/EMS," accessed September 21, 2017, http://scadahistory.com/index.html; Gordon Friedlander, "Computer-Controlled Power Systems: Part II—Area Controls and Load Dispatch," *IEEE Spectrum* 2, no. 5 (May 1965): 72–91; J. N. Boucher, "Real-Time Energy Control" (paper presented at the 1979 Power Industry Computer Applications Conference, Cleveland, OH), 177–184.

220. Cohn, "Recollections," 157–159; Friedlander, "Computer-Controlled Power Systems," 72–89. On the development of economic dispatch techniques

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

and computers, see E. D. Early, W. E. Philips, and W. T. Shreve, "An Incremental Cost of Power-Delivered Computer," *Transactions of the American Institute of Electrical Engineers* 74, no. 3 (1955): 529–535; C. D. Morrill and J. A. Blake, "A Computer for Economic Scheduling and Control of Power Systems," *Transactions of the American Institute of Electrical Engineers* 74, no. 3 (1955): 1136–1142.

221. Martin H. Weik, *A Fourth Survey of Domestic Electronic Digital Computing Systems*, Ballistic Research Laboratories, report no. 1227, January 1964, 89, accessed July 10, 2018, http://ed-thelen.org/comp-hist/BRL64.html#TOC.

222. Ibid.

223. Ibid.

224. On generativity, see Johnathan Zittrain, *The Future of the Internet—and How to Stop It* (New Haven, CT: Yale University Press, 2008).

225. Ibid.

226. *Munn v. Illinois*, 94 U.S.

Chapter 2

1. Richard Nixon, "Remarks on Reform of the Nation's Postal System," September 2, 1969, transcript, The American Presidency Project, https://www.presidency.ucsb.edu/documents/remarks-reform-the-nations-postal-system.

2. Robert B. Simple Jr., "Nixon Again Urges Postal Corporation," *New York Times*, September 3, 1969.

3. See ibid.; "The Halt and the Blind," *New York Times*, July 11, 1969.

4. Lawrence F. O'Brien, *No Final Victories: A Life in Politics from John F. Kennedy to Watergate* (New York: Doubleday, 1974), 210–211.

5. Albin Krebs, "Lawrence O'Brien, Democrat, Dies at 73," *New York Times*, September 29, 1990.

6. O'Brien, *No Final Victories*, 210–211; Baxter, *Labor and Politics*, 83–85.

7. Baxter, *Labor and Politics*, 83–85.

8. O'Brien, *No Final Victories*, 210–211.

9. As quoted in Ted Sell, "Nixon Plea for P.O. Reform," *Boston Globe*, September 3, 1969.

10. O'Brien, *No Final Victories*, 211.

11. Ibid., 210–211.

12. Krebs, "Lawrence O'Brien."

13. On the unexpectedness of deregulation, see Martha Derthick and Paul Quirk, *The Politics of Deregulation* (Washington, DC: Brookings Institution, 1985); Horwitz, *Irony of Regulatory Reform*; Richard H. K. Vietor, *Contrived Competition: Regulation and Deregulation in America* (Cambridge, MA: Belknap Press of Harvard University Press, 1994).

14. See Judt, *Ill Fares the Land*.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

15. Per capita volume growth was just as striking. In 1970 per capita mail volume was 421 for each person in the U.S., compared to 371 in 1965 and 228 in 1930. Gerald Cullinan, *The United States Postal Service* (New York: Praeger, 1973), 2; Fuller, *American Mail*, 334; POD, *Annual Report, 1969*, 236–241, table 801.

16. POD, *Annual Report, 1969*, 236–241, table 801.

17. Congress consistently refused to increase investment in postal infrastructure (in the form of creating new facilities or investing in new technologies to modernize sorting and transportation) through rate increases (which were never popular) or appropriations. For a complete discussion of the relationship between the structure of regulation and mail processing, see chapter 1. The decline in rail service was sharp and challenged the ability of the Post Office to move the mail quickly and efficiently. Post offices had been strategically located adjacent to rail lines in order to assist quick processing and distribution, and railway postal cars provided in-transit sorting. With the decline of rail and the subsequent shift to truck and air, the postal network became increasingly difficult to access, and the railway postal cars became mostly a curiosity. President's Commission, *Towards Postal Excellence: Commission*, 170.

18. Eventually, extra workers were hired, others worked overtime, and the situation was corrected. Kathleen Conkey, *The Postal Precipice: Can the U.S. Postal Service be Saved?* (Washington, DC: Center for the Study of Responsive Law, 1983), 37; President's Commission, *Towards Postal Excellence: Commission*, 11–14.

19. President's Commission, *Towards Postal Excellence: Commission*, 12.

20. Lawrence F. O'Brien, "Lawrence F. O'Brien Oral History Interview XXI," June 18, 1987, interview by Michael L. Gillette, LBJ Library, http://www.lbjlibrary.net/assets/documents/archives/oral_histories/obrien_l/OBRIEN21.PDF.

21. The case for reorganization is provided in the Kappel Commission's report and supplementary documentation. See President's Commission, *Towards Postal Excellence: Commission*; President's Commission on Postal Organization, *Towards Postal Excellence: Report of the General Contractor*, Annex Contractor's Reports, vol. 1–4 (Washington, DC: Government Printing Office [GPO], 1968).

22. Blount only accepted the position of postmaster general on the condition that President Nixon support him in seeking reform. The Citizens Committee for Postal Reform was created at the behest of the Nixon administration to help advance the difficult cause of postal reform. The cochairs of the committee were O'Brien and Thurston Morton, former chairs, respectively, of the Democratic and Republican National Committees. O'Brien, "Lawrence F. O'Brien Oral History"; Robert Saltzstein and Ronald Resh, "Postal Reform: Some Legal and Practical Considerations," *William and Mary Law Review* 12, no. 4 (1971): 766–786; Murray B. Comarow, "The Strange Story of Postal Reform" (Washington, DC: Federal Trade Commission, 2007), accessed June 5, 2013,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

https://web.archive.org/web/20130605181043/http://www.ftc.gov/os/comments/USPS%20Study/529332-00004.pdf.

23. Most notably, during the 1840s private expresses mounted a sustained challenge to the legitimacy and viability of the Post Office. See Priest, "History of the Postal Monopoly," 33–80.

24. POD, *Annual Report, 1969*, 236–241.

25. Richard John and Richard Kielbowicz note the important role that postal rates played in the development of a national market for information and the publishing industry. See John, *Spreading the News*; Kielbowicz, *News in the Mail*. Theda Skocpol notes that the spread of voluntary associations on a national scale mimicked the structure of the federal government and was supported by cheap second-class postage. *Diminished Democracy: From Membership to Management in American Civic Life* (Norman: University of Oklahoma Press, 2003). After Andrew Jackson took office in 1829, the Post Office functioned as an adjunct to the growing national political parties and as a key means of allocating spoils. Postmaster positions, representing each district in the nation, were lucrative (particularly when combined with operating a store or other business) and were an easy way of keeping the political machinery well oiled. John, *Spreading the News*, 206–256; Fuller, *American Mail*, 285–330. Civil service reform and the passage of the Pendleton Act in 1883 did little to separate the connection between the postal bureaucracy and the spoils system. Postmaster positions were exempt from the reform and were still doled out according to political favoritism. For example, Postmaster General Wanamaker replaced over 48,000 of the total 56,315 postmasters during his tenure (1889–1893) in office. Wayne E. Fuller, *RFD: The Changing Face of Rural America* (Bloomington: Indiana University Press, 1964), 86. Clerks and city mail carriers, the bulk of the urban workforce, however, did come under civil service regulation during the early 1900s. Fuller, *American Mail*, 310–330.

26. Special interests played a key role in postal rates and classifications. Importantly, however, these interests were not only external to postal policy but were creations of postal policy. See Kennedy, "Postal Rates."

27. Though challenges were frequent, none was quite as serious as that presented by the private express companies during the middle decades of the 19th century. On how the linkages between the Post Office, political parties, and the publishing industry helped to maintain the unique iteration of postal service, see Priest, "History of the Postal Monopoly"; Richard R. John, "Private Mail Delivery in the United States during the Nineteenth Century: A Sketch," *Business and Economic History* 2, no. 15 (1986): 135–147.

28. Letter carrier unions and voluntary associations were founded in the wake of the creation of free city delivery in 1863. By the early 1960s, the Post Office was one of the most heavily unionized areas of government, with 87.5% of all workers belonging to one of the craft unions. Although these workers could not legally strike, Executive Order No. 10988 in 1962 recognized unions within federal agencies. President's Commission, *Towards Postal Excellence: Commission*, 18–22, 114. A detailed history of the unionization of the postal workforce

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

can be found in Sterling D. Spero, *The Labor Movement in a Government Industry: A Study of Employee Organization in the Postal Service* (New York: Arno, 1971).

29. In 1970 postal workers engaged in a wildcat strike over wages and working conditions that severely affected service. As part of negotiations to end the strike, the unions and administration worked out the deal to secure passage of the PRA. Tierney, *Postal* Service, 15–31; Conkey, *Postal Precipice*, 52–58; President's Commission, *Towards Postal Excellence: Commission*, 102.

30. Postmaster General O'Brien played a key in shaping the ultimate recommendations of the commission. See O'Brien, "Lawrence F. O'Brien Oral History."

31. The Kappel Commission argued that reorganization would reduce postal costs by 20% without having an impact on levels of service. President's Commission, *Towards Postal Excellence: Commission*, 5–6.

32. The commission noted that "only a Post Office quick to identify and meet market needs can successfully serve a changing economy." Ibid., 3.

33. Appropriations were phased out gradually. Currently, appropriations covering "revenue foregone" are only provided for discounted mail for the blind and overseas absentee ballots. See Congressional Research Service, *The Postal Revenue Forgone Appropriation: Overview and Current Issues*, RS21025 (Washington, DC, December 28, 2005).

34. The Board of Governors is composed of nine appointed board members and two further members—the postmaster and deputy postmaster general—who are appointed by the other members of the board.

35. See Tierney, *Postal Service*; Conkey, *Postal Precipice*.

36. Postal Reorganization Act of 1970, Pub. L. No. 91–375 § 3622(b)2–3 (1970).

37. An administrative law judge was used by the U.S. Postal Rate Commission (PRC) to preside over the first two rate cases held after reorganization. Thereafter, the PRC held the hearings directly.

38. Dockets R71-1, R74-1, and R76-1 (PRC) provide exhaustive discussions of the different proposed costing methodologies and their implication for different categories of mailers. PRC, *Postal Rate and Fee Increases, 1971*, No. R71-1 (Washington, DC, 1972); PRC, *Postal Rate and Fee Increases, 1973*, No. R74-1 (Washington, DC, 1975); PRC, *Postal Rate and Fee Increases, 1975*, No. R76-1 (Washington, DC, 1976).

39. Second-class mailers (magazine publishers and newspaper associations) aligned with the Board of Governors against the positioning of cost as the central tenet of rate making. They pointed out the unique value of the content they mailed and the historic support postal rates afforded. Second-class mailers supported the accounting scheme introduced by the board that left a significant (greater than half) portion of total costs assignable and employed inverse elastic pricing as well as an interpretation of value-of-service structured around content.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

40. A partial listing of those costs classified by USPS as "institutional" or common is instructive. In the words of the administrative law judge who oversaw the first two rate cases, broad classification by USPS of institutional costs included "substantially all costs for the purchase and lease of buildings, the purchase and lease of equipment and vehicles, expenses for vehicle drivers, vehicle maintenance, building and equipment maintenance and custodial costs, the cost of a mailman's driving or walking his route to deliver mail, one-third of purchased transportation, most supplies including gasoline and oil, and a considerable portion of clerk's time." Chief administrative law judge Seymour Wenner, in PRC, *Chief Administrative Law Judge's Initial Decision*, No. R71-1 (Washington, DC: PRC, 1971), 8–9.

41. For the various interveners' complaints and claims of discriminatory pricing, see PRC, *Postal Rate and Fee Increases, 1971*, 63–112.

42. Administrative law judge Seymour Wenner presided over the first two rate cases in concert with the PRC. He was very sympathetic to the claims of first-class mailers and challenged the continuation of cross-subsidies, noting disapprovingly: "If someone gets something for nothing someone else pays for it." Wenner, *Initial Decision*, 44.

43. For a summary of the disputes over attributable and assignable costs in the first several cases, see Wenner, *Initial Decision,* 3–17; PRC, *Postal Rate and Fee Increases, 1973*, 1–114; PRC, *Postal Rate and Fee Increases, 1975,* 76–116; U.S. Commission on Postal Service, *Report of the Commission on Postal Service*, vol. 1 (Washington, DC: GPO, 1977), 57–73; John T. Tierney, *Postal Reorganization: Managing the Public's Business* (Boston: Auburn, 1981), 119–134; Tierney, *Postal Service*, 142–171; Conkey, *Postal Precipice*, 205–277.

44. USPS assigned the following percentage of total costs as attributable: R71-1, 49%; R74-1, 45.1%; R76-1, 55.1%. The chief examiner countered in R74-1 by attributing 70.6%, which the PRC modified to 53.5%. In R76-1, the PRC modified the board's figure to 60.4% (see PRC, *Postal Rate and Fee Increases, 1975*, 59–67 and the dockets of each case). During the fourth rate case, which began in 1977, the PRC attributed 74.5% of costs, in agreement with the board. Tierney, *Postal Reorganization*, 130; Tierney, *Postal Service*, 162.

45. The National Association of Greeting Card Publishers filed a lawsuit in 1975 challenging the discretionary authority of the board to determine costing methodology and assign rates (apportion institutional costs). The case eventually was joined with a similar challenge from UPS and progressed to the Supreme Court. In *National Association of Greeting Card Publishers, et al. v. United States Postal Service* (1983), the court upheld the authority of the board to use discretion in setting rates. In other words, full-cost accounting was not necessary. But by this time, first- and third-class mailers (along with private delivery firms) had already succeeded in pushing for a greater amount of cost attribution, successfully challenged the system of cross-subsidies, and attacked content-based assessments of value. Despite the victory for the Board of Governors, the basic terms of service were already radically transformed. National

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Association of Greeting Card Publishers, et al. v. United States Postal Service, 462 U.S. 810 (1983).

46. Implicitly and explicitly, the challenge to the authority of the Board of Governors to use discretion to assign costs was linked with a narrow view of value. Wenner, echoing the sentiments of those seeking to reduce the freedom of the Board of Governors, stated: "Value of service considerations should in the main deal with demand factors. The demand for a class reflects the evaluation placed by both the sender and recipient." Wenner, *Initial Decision,* 15. This opinion is a radical rebuke to the way in which postal policy had been viewed for well over a century. In viewing value so narrowly, Wenner was arguing that postal service and indeed communication have little public value and instead are only significant as a matter between two contracting parties. A general disdain for evaluations of content is repeated throughout his opinions in R71-1 and R74-1. The PRC similarly adopted this dim view of content-related considerations of value in R76-1 but did not go so far as to say that the use of discretion was, in and of itself, discriminatory. PRC, *Postal Rate and Fee Increases, 1975*, 75–156. Many decried this development, noting that it would help hasten the decline of small, marginal publications. Arthur Schlesinger Jr. saw that rising second-class rates had transformed USPS into the "judge, jury, and executioner of the nation's intellectual life" (as quoted in Tierney, *Postal Reorganization*, 129). A June 16, 1975, *Time* magazine editorial also argued that the shifting of costs from first- to second-class mail would irrevocably damage small, marginal publications. It noted that second-class rates had increased over 100% since 1971 and that greater increases were forthcoming. "Postal Nightmare," *Time*, June 16, 1975.

47. The new hostility toward the reallocation of costs was expressed most clearly by Wenner. In his opinion in R74-1, he wrote: "The Postal service has become a tax-collecting agency, collecting money from first-class mailers to distribute to other favored classes" and that this situation had to be undone as quickly as possible. PRC, *Chief Administrative Law Judge's Initial Decision*, No. R74-1 (Washington, DC: PRC, 1973), 13. Antitrust principles have been applied to the Post Office's parcel delivery service since the inception of parcel post.

48. The Postal Accountability and Enhancement Act provides a further elaboration of these principles by dividing postal operations between competitive and market-dominant lines and calling for greater cost attribution and limitation on cross subsidies. Postal Accountability and Enhancement Act, Pub. L. No. 109–435, 120 Stat. 3198 (2006).

49. Presorting discounts were first suggested by Readers Digest Corporation and the Association of Public Utility Mailers (APUM) during the 1971 rate case and were given a separate classification hearing in 1973. PRC, *Opinion and Recommended Decision*, No. MC73-1 (Washington, DC: PRC, 1976), 11. For the initial call, see PRC, *Postal Rate and Fee Increases, 1971*, 112–120. The postal unions, such as the American Postal Workers Union, repeatedly challenged that these rates offer discounts above cost avoidance and transfer productivity gains to particular users at the expense of the general system. For an overview of the history of these categories and critiques of their effectiveness,

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

see GAO, *US Postal Service: A Primer on Postal Worksharing*, GAO-03–927 (Washington, DC, 2003).

50. Estimates during the 1970s suggested that roughly 14% of total first-class mail volume, the bulk of which consisted of checks and bills, could be diverted due to EFT by 1985. EMS was seen as a more long-term threat. USPS briefly considered but discarded extending the letter monopoly into electronic communications on the grounds that it was untenable. Rather, USPS sought to enter the electronic communications market as one of multiple providers. On the challenge posed by new forms of electronic communication, see USPS, *The Private Express Statutes and Their Administration* (Washington, DC: GPO, 1973); Commission on Postal Service, *Report*, vol. 1–2; U.S. Department of Commerce, *The Postal Crisis: The Postal Function as a Communications Service* (Washington, DC: GPO, 1977); PRC, *Opinion and Recommended Decision*, No. MC78-3 (Washington, DC: PRC, 1979); U.S. Office of Technology Assessment (OTA), *Implications of Electronic Mail and Message Systems for the US Postal Service*, OTA-CIT-184 (Washington, DC: OTA, 1982); OTA, *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity*, OTA-BP-CIT-12 (Washington, DC: OTA, 1982).

51. The PRC held open hearings, similar to a rate case, that weighed the merits of E-COM and were collected in PRC, *Mail Classification Schedule, Proposal 1978*, No. MC78-3 (Washington, DC: PRC, 1979).

52. PRC, *Opinion and Recommended Decision*, MC78–3, 24–30.

53. E-COM was supported by President Carter and the postal Board of Governors as a way of extending and expanding postal service. See "Administration's Policy Statement July 19, 1979," app. B, in James Duffy, *Dissenting Opinion and Recommended Decision*, No. MC78-3 (Washington, DC: PRC, 1979). The statement reads in part: "As long as physical delivery through the mails exists as a primary means of communications to a large segment of the population, USPS should take advantage of electronic communications to improve its service." The Board of Governors, the PRC, and the congressionally created Commission on Postal Service (created to review postal service) all concluded that integrating "electronic mail" and traditional letter mail was advisable. Duffy, *Dissenting Opinion*, MC78-3; PRC, *Mail Classification Schedule*, *Proposal 1978*; Commission on Postal Service, *Report*, vol. 1.

54. For a larger consideration of E-COM's failure, see Ryan Ellis, "The Premature Death of Electronic Mail: The United States Postal Service's E-COM Program, 1978–1985," *International Journal of Communication* 7 (2013): 1949–1967.

55. The complaints of the interveners are included in preconference statements in the record of MC78-3 and in app. A of the Federal Communications Commission (FCC) declaratory ruling at the request of Graphnet. PRC, *Mail Classification Schedule*, *Proposal 1978*; Graphnet Sys., Inc., 73 F.C.C. 2d 283 (1979).

56. The move to prevent cross-subsidies (particularly from first-class mail rates to E-COM) colors the entirety of the PRC's initial decision (1979) and reconsidered opinion (1980). PRC, *Opinion and Recommended Decision*, MC78-3;

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

PRC, *Opinion and Recommended Decision upon Reconsideration*, No. MC78-3 (Washington, DC: PRC, 1980).

57. The stinging dissenting opinions of Chairmen Duffy and Kieran O'Doherty make this point plain. Duffy notes that despite adopting the Board of Governors' terminology, "a careful reading of the majority opinion will reveal its true intent—to preclude Postal Service entry into electronic mail and to permanently trap the service in a subordinate role from which it cannot escape. … It has recommended a data-processing, envelope-stuffing service, not an electronic mail service; [it] has rejected rather than accepted the concept of electronic mail service; [it] has contrived to postpone rather than encourage electronic mail service; [it] has done so by concealing rather than revealing the true important distinction." O'Doherty's dissent was no less forceful, noting that "the opinion issued by the majority today is a brazen attempt to arrogate the basic powers and responsibilities expressly reserved by statute for the management of the postal Service. … It is a bold rejection of the Postal Service's primary role in the development of new mail services for the American Public." Duffy, *Dissenting Opinion*, MC78-3, 21; Kieran O'Doherty, *Dissenting Opinion and Recommended Decision*, No. MC78-3 (Washington, DC: PRC, 1979), 1.

58. PRC, *Opinion and Recommended Decision*, MC78-3," 1–59, 269–283.

59. In the first six months of operation, 660,000 messages were sent. But by July, E-COM was handling 172,000 messages weekly. OTA, *Implications*, 12.

60. The basic dispute between the PRC and the Board of Governors concerned determining when to recover the costs of investment. The PRC decided, in midstream, to move the test-year period from 1987 to 1985, causing rates to skyrocket. The PRC called for E-COM rates that would have risen from 26 cents to 52 cents for the first page. See PRC, *Opinion and Recommended Decision*, No. R83-1 (Washington, DC: PRC, 1984); PRC, *Opinion and Recommended Decision, upon Reconsideration*, No. R83-1 (Washington, DC: PRC, 1984); James Duffy, *Dissenting Opinion and Recommended Decision*, No. R83-1 (Washington, DC: PRC, 1984), 1–23.

61. *Decision of the Board of Governors of the United States Postal Service Concerning the Opinions and Recommended Decisions for E-COM Rate and Classification Changes*, No. R83-1 (Washington, DC: PRC, 1984).

62. Cortada, *Digital Hand*, 169; Biggart, "Post Office as a Business," 487; POD, *Postal Progress*, 7.

63. GAO, *Postal Service: Information on the Change to Multiline Readers for the Zip + 4 Program*, GAO/GGD-8862BR (Washington, DC, 1986), 31.

64. President's Commission, *Towards Postal Excellence: Commission*, 27–28.

65. GAO, *Conversion to Automated Mail Processing Should Continue; Nine Digit Zip Code Should Be Adopted If Conditions Are Met*, GAO/GGD-83–24 (Washington, DC, 1983), 2.

66. GAO, *Postal Service: Automation Is Taking Longer and Producing Less than Expected*, GAO/GGD-93–89BR (Washington, DC, 1997), 10.

67. Ibid.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

68. GAO, *Automation Is Restraining*, 11.

69. DPS was first used in 1991. GAO, *Automation Is Taking Longer*, 10.

70. Figure calculated from data in Little, "Description of the Postal Service"; GAO, *Automation Is Restraining*, 10.

71. Little, "Description of the Postal Service."

72. GAO, *Automation Is Restraining*, 10–12.

73. By 2006, these figures would continue to improve to 306,034 pieces per career employee. Data from Cortada, *Digital Hand*, 166; USPS, "Statistics: Pieces and Post Offices," in *Postal Service: An American History*.

74. Data from Cortada, *Digital Hand*, 166; USPS, "Statistics: Pieces"; U.S. Census Bureau, *Statistical Abstract of the United States, 2004–2005* (Washington, DC: GPO, 2005), table 1112.

75. The adoption of mechanized equipment before reorganization was limited. President's Commission, *Towards Postal Excellence: Commission*, 24.

76. As of 2003, 13% of postal employees were noncareer workers. From 1980 to 2003, temporary labor increased by 292% (from 25,000 to 98,000), while during the same period career employees increased by only 13% (from 643,000 to 729,000). USPS repeatedly affirms its commitment to reduce costs through a smaller labor force and the deployment of temporary staff. Census Bureau, *Statistical Abstract*, table 1112.

77. GAO, *Automation Is Restraining*, 10–12; USPS, *United States Postal Service Transformation Plan* (Washington, DC, 2002).

78. Data from Cortada, *Digital Hand*, 166; USPS, "Statistics: Pieces." Prices calculated with "Inflation Calculator," U.S. Bureau of Labor Statistics, http://www.bls.gov/data/inflation_calculator.htm.

79. GAO, *Postal Service: Planned Benefits of Iowa Automated Mail Facility Not Realized*, GAO/GGD-94–78 (Washington, DC, 1994), 1.

80. The number of post offices faced a sharp decline in the early part of the 20th century with the introduction of the automobile. Since reorganization, the number of post offices has hovered around 30,000, with little change. The PRA specified that no post office could be closed due to an operating deficit. USPS instituted a moratorium on closing small rural post offices between 1998 and 2002. Robert H. Cohen et al., "The Conflict about Preserving Small Rural Post Offices: Differences in the Distribution of Pharmacies and Post Offices" (paper presented at Winton M. Blount Symposium on Postal History, Washington, DC, November 2006).

81. President's Commission, *Towards Postal Excellence: Commission*, 170–171.

82. USPS, *US Postal Service Emergency Preparedness Plan for Protecting Postal Employees and Postal Customers from Exposure to Biohazardous Material and for Ensuring Mail Security against Bioterror Attacks* (Washington, DC, 2002), app. A, H-1.

83. The postal system as of 2001 contained 350,000 collection boxes and 134.5 million delivery points serviced by a network of nearly 40,000 post offices.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

USPS, *2001 Comprehensive Statement on Postal Operations* (Washington, DC, 2001), 51; USPS, *Emergency Preparedness Plan*, 1–4.

84. Figures are approximate and current to the fall of 2001. USPS, *Emergency Preparedness Plan*, 1–3.

85. For example, the Brentwood facility provides all incoming and outgoing mail processing for Washington, DC (zip codes 20000–20099), connects with 56 local USPS facilities (including branch post offices and stations), and serves 177 different federal facilities. "Anthrax in the U.S. Postal System: Lessons That Stunned Us," Centers for Disease Control and Prevention, last modified 2002, accessed September 25, 2017, ftp://ftp.cdc.gov/pub/infectious_diseases/iceid/2002/pdf/pearson.pdf.

86. Albert Hirschman provides an apt conceptual framework for thinking about how the weakening of the letter monopoly through the introduction of new communication options, the restriction of USPS entry to electronic communication, and the circumscription of the public bureaucracy in the design of rates and classification amounts to the relative elevation of large-volume mailers in the provision of postal service. In his terms, these changes increased the possibility that large mailers could now exit the system. This makes the voice of these groups credible, more significant, and difficult to ignore. As he notes: "The *effectiveness* of the voice option is strengthened by the possibility of exit" (83). His analysis and characterization of the Post Office as a "lazy monopolist," however, is lacking. Its laziness is less a function of its own initiative than the interventions of particular parties. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Cambridge, MA: Harvard University Press, 1970), 59–60, 82–105. On the dire condition that peak volume signals, see President's Commission on the United States Postal Service, *Embracing the Future: Making the Tough Choices to Preserve Universal Service* (Washington, DC, 2003); USPS, *Transformation Plan*.

87. The limits of hub-and-spoke architecture in the face of nonrandom disruptions are outlined in Albert, Jeong, and Barabási, "Error and Attack Tolerance." See also chapter 1.

88. For a detailed discussion, see chapter 1.

89. For a clear discussion of the railroads' proffering of key support for the ICC, see Samuel P. Huntington, "The Marasmus of the ICC: The Commission, the Railroads, and the Public Interest," *Yale Law Journal* 61, no. 4 (1952): 467–509.

90. James C. Nelson, "The Effects of Entry Control in Surface Transport," in *Transportation Economics*, (New York: Columbia University Press, 1965), 381–422; Hoogenboom and Hoogenboom, *History of the ICC*.

91. Hoogenboom and Hoogenboom, *History of the ICC*, 118.

92. On the difficulty of maintaining cross-subsidies in the face of opportunities for bypass, see Horwitz, *Irony of Regulatory Reform*, 7–8.

93. Hoogenboom and Hoogenboom, *History of the ICC*, 146; Stone, *Interstate Commerce Commission*, 39; Levin, "Regulation"; Dennis W. Carlton and

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Randal C. Picker, "Antitrust and Regulation," in *Economic Regulation and Its Reform: What Have We Learned?*, ed. Nancy L. Rose (Chicago: University of Chicago Press, 2014), 25–61.

94. Hoogenboom and Hoogenboom, *History of the ICC*, 129–131; Carlton and Picker, "Antitrust and Regulation"; Nelson, "Effects of Entry Control"; Huntington, "Marasmus of the ICC."

95. Hoogenboom and Hoogenboom, *History of the ICC*, 129–131; Nelson, "Effects of Entry Control"; Kriebel and Baumel, "Freight Transportation Regulation."

96. Hoogenboom and Hoogenboom, *History of the ICC*, 146; Stone, *Interstate Commerce Commission*, 39.

97. GAO, *Railroad Regulation*, 12.

98. Ibid.

99. Association of American Railroads (AAR), *The Impact of the Staggers Rail Act of 1980* (Washington, DC, 2010), accessed November 3, 2010, https://web.archive.org/web/20101103064437/http://aar.org/~/media/aar/backgroundpapers/impactofthestaggersrailactof1980.ashx/; Laurits R. Christensen Associates, *Description of the U.S. Freight Rail Industry*, vol. 1, *Analysis of Competition, Capacity, and Service Quality*, prepared for the Surface Transportation Board (Washington, DC, November 2009, 2-2.

100. GAO, *Railroad Regulation*, 12.

101. AAR, "A Short History of U.S. Freight Railroads," August 2017, https://www.aar.org/BackgroundPapers/A%20Short%20History%20of%20US%20Freight%20Railroads.pdf; GAO, *Railroad Regulation*; Levin, "Regulation."

102. The failure of specific railroads presented a more general problem. The railroad network is interdependent, and freight moves across and between different carriers through exchanges to reach its end point. Thus, the failure of a sizable carrier has effects that impair the larger network. Gaskins, "Regulation of Freight Railroads"; GAO, *Railroad Regulation*, 11.

103. These committees, formed under the guidance of the Council of Economic Advisors, released a "Bicentennial Bill of Rights for Railroads" on the nation's bicentennial. Stone, *Interstate Commerce Commission*, 54–55, 85.

104. See, e.g., Meyer et al., *Economics of Competition*; James C. Nelson, *Railroad Transportation and Public Policy* (Washington, DC: Brookings Institution, 1959); George W. Hilton, *The Transportation Act of 1958: A Decade of Experience* (Bloomington: Indiana University Press, 1969); Friedlaender, *Dilemma*. For an overview of studies during this period, see Stone, *Interstate Commerce Commission*, 48–50.

105. John D. Bitzan and Theodore E. Keeler, "Economies of Density and Regulatory Change in the U.S. Railroad Freight Industry," *Journal of Law and Economics* 50, no. 1 (2007): 173.

106. Nelson, "Effects of Entry Control," 414.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

107. Robert C. Fellmeth, *The Interstate Commerce Omission: The Public Interest and the ICC* (New York: Grossman, 1970). See also Stone, *Interstate Commerce Commission*, 50.

108. Kolko, *Railroads and Regulation*.

109. The Landis report prepared for President-Elect Kennedy in 1960 offered a strong critique of the regulatory agencies, and Congress issued the similarly stinging Doyle Report of the Senate Transportation Study Group in 1961. In 1962, President Kennedy issued a special Transportation Message to Congress, arguing that current regulations were "a chaotic patchwork of inconsistent and often obsolete legislation" in need of reform. Stone, *Interstate Commerce Commission*, 48–54.

110. Ibid., 78–80.

111. See Derthick and Quirk, *Politics of Deregulation*.

112. Hoogenboom and Hoogenboom, *History of the ICC*, 178–179; Stone, *Interstate Commerce Commission*, 76.

113. Stone, *Interstate Commerce Commission*, 77–78.

114. Ibid., 88–90.

115. Stone, *Interstate Commerce Commission*, 113–141; GAO, *Railroad Regulation*, 15; Gaskins, "Regulation of Freight Railroads"; Bitzan and Keeler, "Economies of Density," 157–179; Ming-Jeng Hwang and Patrick C. Mann, "Deregulation and Efficiency in the Rail Industry," *Atlantic Economic Journal* 15, no. 2 (1987): 47–52; Elizabeth E. Bailey, "Price and Productivity Change Following Deregulation: The US Experience," *Economic Journal* 96, no. 381 (1986): 1–17.

116. 4(R) also attempted to speed up the abandonment process. Stone, *Interstate Commerce Commission*, 97.

117. AAR, "Overview of America's Freight Railroads," August 2017, https://www.aar.org/BackgroundPapers/Overview%20of%20America's%20Freight%20RRs.pdf; Rodrigue, Comtois, and Slack, *Geography of Transport Systems*.

118. The dramatic consolidation of Class I railroads also followed Staggers. In 1980 there were 40 Class I railroads; two decades later there were 7. Carlton and Picker, "Antitrust and Regulation," 46–48; AAR, "Overview of America's Freight Railroads."

119. In concert with the relaxation of abandonments, after 1980 the ICC moved to eliminate Detroit, Toledo, and Ironton conditions (DT&I), which compelled railroads to preserve patterns of freight movement in the wake of mergers. Gaskins, "Regulation of Freight Railroads."

120. Significant savings came from reductions in labor as well as the elimination of unprofitable track. Carlton and Picker, "Antitrust and Regulation."

121. The use of contract rates helped, in part, to drive the decline in rates. By 1988, 60% of all Class I freight moved under contract rates. AAR, "Overview of America's Freight Railroads"; Stone, *Interstate Commerce Commission*, 161.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

122. Data from AAR, "Impact of the Staggers Rail Act of 1980"; Christensen Associates, *Freight Rail Industry*, 2-2.

123. Data from "A Short History of U.S. Freight Railroads."

124. For a detailed discussion of the impact of deregulation on density, see Bitzan and Keeler, "Economics of Density."

125. Ibid., 173–175.

126. After Staggers, during the 1990s, the Department of Transportation (DOT) reconfigured how to tabulate commodity flow after surveys during the 1980s were considered incomplete and abandoned due to quality concerns. As part of this reconfiguration, the economic census now provides fairly detailed and specific information about commodity flow.

127. GAO, *Railroad Regulation*, 53; H. Barry Spraggins, John Ozment, and Phillip Fanchon, "Risk Modeling of Hazardous Materials Rail Movement to Include a Terrorist Incident," *Journal of the Academy of Business and Economics 5*, no. 3 (2005); AAR, "Overview of America's Freight Railroads."

128. Note, updated figures from the 2017 *Commodity Flow Survey* are not yet available. Bureau of Transportation Statistics, "Hazardous Materials," in DOT, *Commodity Flow Survey*, February 2015, tables 1a, 6.

129. Commodity flow data from the economic census are not available for the 1980s. Additionally, the categories listed changed in the mid-1990s, making direct comparisons between eras difficult (for example, in the 1990s flow data about hazardous materials were collected, while in the 1960s and 1970s no such data were collected). However, the basic picture indicated—of increasing rail volume and increasing shares of transported commodities both generally and for dangerous materials—appears to be valid. In 1993, when data and categories comparable to those used in previous surveys were last employed, rail carried 59.9% of total ton-miles for industrial chemicals, compared with just 20.7% carried by truck. This shows a reversal of the trend observed during the 1960s and 1970s, when rail's share declined from a high of 67.1% to 57.4%, and truck increased its share from a low of 15.6% to 24.9%. Ibid.; DOT, *1993 Economic Census* (Washington, DC, 1996); Census Bureau, *Commodity Transportation Survey*.

130. See Brown, Dunn, and Policastro, *National Risk Assessment*.

131. Similar figures hold for TIH materials. TIH shipments via rail travel in 90-ton tanker trucks and travel, on average, 480 miles. Transportation Research Board, *Cooperative Research*, 19; Bureau of Transportation Statistics, "Hazardous Materials," tables 1a, 6; Brown, Dunn, and Policastro, *National Risk Assessment*.

132. Statistics show that 99.9% of all rail shipments arrive without incident. AAR, "Railroads the Safe Way to Move," March 2005, accessed July 10, 2012, http://www.aar.org/pubcommon/documents/policy/safe_way_to_move.pdf.

133. Brown, Dunn, and Policastro, *National Risk Assessment*, 4, 179.

134. Ibid., 148–150.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

135. For an extensive discussion of the cross modal comparisons of the risks of transporting hazardous materials and TIH materials, see ibid.

136. Eben Kaplan, *Rail Security and the Terrorist Threat* (New York: Council on Foreign Relations, 2007), http://www.cfr.org/united-states/rail-security-terrorist-threat/p12800.

137. For a discussion of the details of the Graniteville, South Carolina, accident and others, see Lewis M. Branscomb et al., "Rail Transportation of Toxic Inhalation Hazards: Policy Responses to the Safety and Security Externality" (working paper RPP-2010-01, Mossavar-Rahmani Center for Business & Government Regulatory Policy Program, Harvard University, 2010), http://www.hks.harvard.edu/m-rcbg/rpp/Working%20papers/Rail%20Transportation%20of%20TIH.pdf.

138. For a discussion of population density and the risk of hazardous materials transportation, see Brown, Dunn, and Policastro, *National Risk Assessment*.

139. Hirsh, *Power Loss*, 1.

140. The grow-and-build strategy was not particular to the postwar era. Samuel Insull's machinations to increase load factors during the early 20th century set out to accomplish the same results. See chapter 1 for a discussion of Insull. See also Hirsh, *Power Loss*, 46; Hirsh, *Technology and Transformation*, 19–21.

141. Recall, as noted in chapter 1, that the structure of rate-of-return regulation rewarded investment in new technologies.

142. During the late 1940s, plants converted roughly 22% of a fuel's content to energy, but by the 1960s advances in steam temperatures and turbines allowed plants to operate with a thermal efficiency of 33%. Hirsh, *Power Loss*, 56.

143. Capacity of the largest units jumped from 190 MW to 575 MW between 1950 and 1960, while the average cost of new plant construction dropped from $173 per kilowatt-hour to $149 per kilowatt-hour in adjusted dollars. Ibid.

144. Ibid., 47.

145. Industrial prices, always lower than residential rates, fell to four cents in 1969. Ibid., 47; U.S. Energy Information Administration (EIA), "Average Retail Prices of Electricity, 1960–2012," in *Annual Energy Review* (Washington, DC: Department of Energy, 2017), table 8.10, https://www.eia.gov/totalenergy/data/annual/.

146. Daniel Czamanski, *Privatization and Restructuring of Electricity Provision* (Westport, CT: Praeger, 1999), 88.

147. The declining cost of electricity and the booming market for new electrical appliances helped household consumption spike 150% per household from 1945 to 1965. The growth in output increased over fivefold, from 296.1 billion kWh in 1949 to 1,535.1 billion kWh in 1970. Hirsh, *Power Loss*, 47; Czamanski, *Privatization and Restructuring*, 83; EIA, "Electricity Net Generation: Total (All Sectors) 1949–2012," in *Annual Energy Review*, table 8.2a.

148. Hirsh, *Technology and Transformation*, 85–86.

149. Hirsh, *Power Loss*, 1; Hirsh, *Technology and Transformation*, 82–86.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

150. Hirsh and others identify these three factors as the root causes of the revisiting of utility policy and the eventual introduction of limited competition through PURPA. See Hirsh, *Power Loss*; Czamanski, *Privatization and Restructuring of Electricity Provision*; James L. Sweeney, *The California Energy Crisis* (Stanford, CA: Hoover Institution, 2002); Beder, *Power Play*.

151. Metallurgical problems in boilers and turbines appeared as thermal efficiencies approached rates of 40% and presented real limitations to improved operation. New 1,300 MW units came online in the late 1960s and early 1970s and presented reliability problems. Hirsh, *Power Loss*, 55–58; Hirsh, *Technology and Transformation*, 89–99.

152. The Organization of Petroleum Exporting Countries (OPEC), in retaliation for support of Israel in the Yom Kippur War, cut oil production, increased prices, and subsequently embargoed oil shipments to the U.S.

153. Petroleum prices fell 30% between 1957 and 1970. Hirsh, *Power Loss*, 60.

154. Ibid.

155. Ibid., 61.

156. Ibid., 64–65.

157. Michael Schudson, *The Rise of the Right to Know: Politics and the Culture of Transparency, 1945–1975* (Cambridge, MA: Belknap Press of Harvard University Press, 2015).

158. Ibid., 170–175.

159. Regulatory commissions, long deferential to utilities, began in some instances to deny cost recovery and proposed projects. The Environmental Defense Foundation (EDF) won a major victory during the 1976 California Public Utilities Commission's review of a proposed Pacific Gas & Electric (PG&E) nuclear plant by introducing alternate demand forecasts based on conservation. Ultimately, PG&E incorporated some of the EDF's suggestions and scrapped the planned project. The EDF's victory was not an isolated event. Hirsh, *Technology and Transformation*, 151–152; Hirsh, *Power Loss*, 64–68.

160. Imported petroleum accounted for an increasing share of domestic consumption. In 1973 imported petroleum accounted for 36% of domestic consumption, but by 1976, imports accounted for 42% and showed signs of increasing growth. The plan included taxes and incentives in favor of conservation, nuclear power, and coal; the granting of new federal power to force utility interconnection; and the end of the promotional block rate structure. Ibid., 73–75.

161. Ibid., 73–80.

162. Section 210, which turned out to be the key provisions of PURPA, was overlooked during the debate. Ibid., 81–88.

163. QFs were defined as renewable power producers under 80 MW and cogeneration facilities of any size. FERC, "What Is a Qualifying Facility?," last modified November 18, 2016, http://www.ferc.gov/industries/electric/gen-info/qual-fac/what-is.asp; Sweeney, *California Energy Crisis*, 11–15; Hirsh, *Power*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Loss, 81–88; Paul L. Joskow, "Deregulation and Regulatory Reform in the US Electric Power Sector," in *Deregulation of Network Industries: What's Next?*, ed. Sam Peltzman and Clifford Winston (Washington, DC: Brookings Institution, 2000), 126.

164. They controlled a monopsony market within which they were the only buyer.

165. Hirsh, *Power Loss*, 81–88.

166. Ibid., 81–82.

167. Ibid., 87.

168. QFs could buy power at residential rates from utilities, which were based on average costs that were significantly less than avoided costs, and then turn around and sell power back to utilities at higher rates based on avoided costs. Ibid., 86–91.

169. Ibid., 115–116, figs. 6.7 and 6.8.

170. EIA, "Net Generation by State by Type of Producer by Energy Source, 1990–2017," last modified January 15, 2019, http://www.eia.doe.gov/cneaf/electricity/epa/epa_sprdshts.html; Hirsh, *Power Loss*, 114; Paul L. Joskow, "The Difficult Transition to Competitive Energy Markets," in Griffin and Puller, *Electricity Deregulation*, 47.

171. Hirsh, *Power Loss*, 123; Joskow, "Deregulation and Regulatory Reform," 126.

172. Hirsh, *Power Loss*, 123; Joskow, "Deregulation and Regulatory Reform," 126; Sweeney, *California Energy Crisis*, 15–16.

173. Hirsh, *Power Loss*, 119.

174. The Edison Electric Institute/Alliance of Energy Suppliers would push for deregulation, while entrenched utilities (IOUs) formed the Electric Reliability Coalition to fight the opening of transmission and distribution networks to competition. Beder, *Power Play*, 88; Hirsh, *Power Loss*, 245.

175. Joskow, "Deregulation and Regulatory Reform," 126.

176. Ibid.

177. Hirsh, *Power Loss*, 241–245; Sweeney, *California Energy Crisis*, 17; Joskow, "Deregulation and Regulatory Reform," 138; Griffin and Puller, "Introduction," 3.

178. Paul L. Joskow, "Restructuring, Competition and Regulatory Reform in the U.S. Electricity Sector," in *Designing Competitive Electricity Markets*, ed. Chao Hung-Po and Hillard G. Huntington (Boston: Kluwer, 1998), 11-31.

179. Hirsh, *Power Loss*, 244–245; Joskow, "Restructuring"; Beder, *Power Play*, 87–88.

180. "The Energy Policy Act of 1992," EIA, accessed September 27, 2017, http://www.eia.doe.gov/oil_gas/natural_gas/analysis_publications/ngmajorleg/enrgypolicy.html.

181. Hirsh, *Power Loss*, 241–244.

182. Ibid., 243.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

183. By 2007, non-utility capacity accounted for 42% of capacity. Among utilities, IOUs accounted for 37.69% of capacity, while cooperatives and federal and public utilities accounted for an estimated 20%. See EIA, "Electric Power Industry Overview: 2007," fig. 3, last accessed September 27, 2017, http://www.eia.doe.gov/cneaf/electricity/page/prim2/toc2.html; EIA, "Net Generation by State."

184. EIA, *Electric Power Annual 2009* (Washington, DC: Department of Energy, 2011), 53, table 6.2, https://www.eia.gov/electricity/annual/archive/03482009.pdf; EIA, "Net Generation by State."

185. FERC, "What Are the Benefits of QF Status," last accessed August 22, 2018, https://www.ferc.gov/industries/electric/gen-info/qual-fac/benefits.asp.

186. FERC, Order No. 888, *Promoting Wholesale Competition through Open Access Non-discriminatory Transmission Services by Public Utilities and Recovery of Stranded Costs by Public Utilities and Transmitting Utilities*, 75 F.E.R.C. ¶ 61,080 (1996) (to be codified at 18 C.F.R. pts. 35, 385); FERC, Order No. 889, *Open Access Same-Time Information System (formerly Real-Time Information Networks) and Standards of Conduct*, 75 F.E.R.C. ¶ 61,078 (1996) (to be codified at 18 C.F.R. pt. 37); FERC, Order No. 2000, *Regional Transmission Organizations*, 89 F.E.R.C. ¶ 61,285 (1999) (to be codified at 18 C.F.R. pt. 35).

187. Under the Energy Policy Act, FERC now has the power to order utilities to open transmission facilities to independent producers (interconnection), even if such an extension requires the expansion of transmission facilities. Joskow, "Deregulation and Regulatory Reform," 129–133; Hirsh, *Power Loss*, 244.

188. Joskow, "Deregulation and Regulatory Reform," 131–132; Richard F. Hirsh, "Restructuring or Deregulation?," *Understanding Deregulation*, Smithsonian Institute, last modified June 2012, http://americanhistory.si.edu/powering/dereg/dereg1a.htm.

189. *ISO* and *RTO* are used interchangeably by FERC, though RTOs historically have been multistate in nature. ISO/RTOs oversee what are known as *organized markets*, as opposed to markets lacking a central coordinator/operator, which are organized through bilateral contracts. U.S. Government Accountability Office (GAO), *Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance*, GAO-08–987 (Washington, DC, 2008), n3; ISO/RTO Council, *2009 State of the Markets Report* (Washington, DC, 2009), http://www.isorto.org/Documents/Report/2009IRCStateOfTheMarketsReport.pdf.

190. ISO/RTO Council, *2010 ISO/RTO Metrics Report* (Washington, DC, 2010), 9–26, http://www.isorto.org/Documents/Report/2010IRCMetricsReport_2005-2009.pdf; GAO, *Electricity Restructuring*, 2–3; "Electric Power Industry Overview: 2007."

191. With one exception: ERCOT only operates within the state of Texas and is overseen by the state utility commission.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

192. Current ISO/RTOs in operation: California ISO, Southwest Power Pool, Midwest ISO, New York ISO, ISO New England, PJM Interconnection, and the Electric Reliability Council of Texas (ERCOT). ERCOT, unlike the other ISO/RTOs, operates under Texas state laws, rather than FERC jurisdiction. "Electric Power Industry Overview: 2007"; ISO/RTO Council, *2010 ISO/RTO Metrics Report*.

193. In those areas not served by ISO/RTOs, competitive wholesale markets operate through bilateral contracts. ISO/RTO Council, *2010 ISO/RTO Metrics Report*, 11; ISO/RTO Council, "IRC Brings Value to Reliability and Electricity Markets," accessed March 28, 2010, http://www.isorto.org/site/c.jhKQIZPBImE/b.2603917/k.B00F/About.htm; EIA, *Electric Power Annual 2009*, 4, fig. ES2; ERCOT, "ERCOT Quick Facts," last modified July 2010, http://www.ercot.com/content/news/presentations/2010/ERCOT%20Quick%20Facts%20-%20July%202010.pdf.

194. GAO, *Electricity Restructuring*, 2–3; ISO/RTO Council, *2010 ISO/RTO Metrics Report*; ISO/RTO Council, *Markets Report*.

195. As noted in chapter 1, electric power, due to its unique characteristics, requires real-time control and coordination to balance demand and supply. Electricity does not move through interconnected networks in a point-to-point, switched fashion but rather moves according to Kirchhoff's laws and requires that total generation and consumption must be balanced. ISO/RTOs now are entrusted to provide reliability through balancing, dispatch, and real-time system monitoring. Joskow, "Deregulation and Regulatory Reform," 116; ISO/RTO Council, *2010 ISO/RTO Metrics Report*; ISO/RTO Council, *Markets Report*.

196. Cohen, Grid, 126.

197. Electric Reliability Council of Texas, "History," http://www.ercot.com/about/profile/history/; ISO/RTO Council, *2010 ISO/RTO Metrics Report*, 145, accessed September 27, 2017, http://www.isorto.org/Documents/Report/2010IRCMetricsReport_2005-2009.pdf.

198. ISO/RTO Council, *2010 ISO/RTO Metrics Report*, 145.

199. See ISO/RTO Council, *Markets Report*; ISO/RTO Council, *2010 ISO/RTO Metrics Report*.

200. ISO/RTO Council, *Markets Report*, 3.

201. Functional unbundling replaced rate-of-return regulation with competitive markets for generation (while leaving rate-of-return regulation in place for transmission and distribution in those areas where retail competition was not introduced).

202. GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04–354 (Washington, DC, 2004), 1–13; Keith Stouffer et al., *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*, special publication 800-82 (Gaithersburg, MD: National Institute

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

of Standards and Technology, 2008), ES-1, 3–1; Ken Barnes, Briam Johnson, and Reva Nickelson, *Review of Supervisory Control and Data Acquisition Systems (SCADA)* (Idaho Falls: Idaho National Laboratory (INL), 2004), 1–3, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.5922&rep=rep1&type=pdf; INL, *National SCADA Test Bed Substation Automation Evaluation Report* (Idaho Falls: INL, 2009), vi–vii, https://inldigitallibrary.inl.gov/sites/sti/sti/4374057.pdf; OE, *National SCADA Test Bed Program: Multi-year Plan, 2008–2013* (Washington, DC: Department of Energy, 2008), https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_OE_NSTB_Multi-Year_Plan.pdf; Energetics Inc., *Roadmap to Secure Control Systems in the Energy Sector*, 2006, 7–8, https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf.

203. U.S. Department of Energy, "Enabling Modernization of the Electric Power System," in *Quadrennial Technology Review: An Assessment of Energy Technologies and Research Opportunities* (Washington, DC, 2015), chap. 3, http://energy.gov/sites/prod/files/2015/09/f26/Quadrennial-Technology-Review-2015_0.pdf.

204. SCADA systems are used in a number of different industries to provide central control and monitoring of remote processes. In electric power, SCADA systems are commonly a part of energy management systems (EMS), which additionally contain automatic generation control (AGC), dispatch, and forecasting systems. Barnes, Johnson, and Nickelson, *Review of SCADA*, 13.

205. SCADA systems are used to monitor distributed processes, while distributed control systems (DCS) are used to monitor and control site-specific operations. DCS are also used in electric power, specifically at generation sites, but are often linked to SCADA systems to provide coordinated control. INL, *SCADA Test Bed Program*, 1; GAO, *Critical Infrastructure Protection: Challenges*, 8–9; Stouffer et al., *Guide to ICS Security*, 2–1.

206. Stouffer et al., *Guide to ICS Security*, 2–1; Barnes, Johnson, and Nickelson, *Review of SCADA*, 13.

207. GAO, *Critical Infrastructure Protection: Challenges*, ES-1, 3–1; Barnes, Johnson, and Nickelson, *Review of SCADA*, 1–3; INL, *National SCADA*, vi–vii; OE, *SCADA Test Bed Program*; Energetics, *Roadmap*, 7–8.

208. Zittrain, *Future of the Internet*.

209. Hirsh, *Technology and Transformation*, 80–82; Anderson, *Regulatory Politics*. See also chapter 1.

210. Indeed, as restructuring unfolded during the 1990s, electric power R&D investment, counted as part of the rate base under rate-of-return regulation, dropped sharply. GAO, *Changes in Electricity-Related R&D*, 3.

211. Barnes, Johnson, and Nickelson, *Review of SCADA*, 2–3; OE, *SCADA Test Bed Program*, 3; Energetics, *Roadmap*, 7–8.

212. The new security challenges introduced by generativity and accessibility are identified and discussed widely. See GAO, *Critical Infrastructure Protection:*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Challenges, 2–13; GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08–119T (Washington, DC, 2007), 6; North American Electric Reliability Corporation, *Long-Term Reliability Assessment: 2009–2018* (Princeton, NJ: NERC, 2009), 67–69; OE, *SCADA Test Bed Program*, 4; Bri Rolston, *Improving Control System Security through the Evaluation of Current Trends in Computer Security Research* (Idaho Falls: Idaho National Engineering and Environmental Laboratory, 2005), 2, https://inldigitallibrary.inl.gov/sites/sti/sti/3395023.pdf; Stouffer et al., *Guide to ICS Security*, 3-15-3-16.

213. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (New York: Cambridge University Press, 2018), 15. Mauer adapts the work of both Lockheed Martin and Assante and Lee. See Lockheed Martin, "Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense," last accessed August 20, 2018, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html; Michael J. Assante and Robert M. Lee, "The Industrial Control System Kill Chain," SANS Institute, October 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

214. Zittrain, *Future of the Internet*.

215. Ibid.

216. Ibid.

217. See Dragos Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," version 2.20170613, last accessed August 20, 2018, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf; Dragos Inc., "Industrial Control System Threats," March 2018, last accessed August 20, 2018, https://www.dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf.

218. See Dragos, CRASHOVERRIDE; Dragos, "Industrial Control System Threats."

219. The limited circulation of information about customized systems limits the community of skilled technicians working to identify flaws and improve reliability.

220. GAO, *Critical Infrastructure Protection: Challenges*, 17; Kevin Paulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," *Security Focus*, August 19, 2003, http://www.securityfocus.com/news/6767.

221. For early reporting on Stuxnet, see Brian Krebs, "Experts Warn of New Windows Shortcut Flaw," *Krebs on Security: In-Depth Security News and Investigation*, July 10, 2010; Mark Clayton, "Stuxnet Malware Is 'Weapon' Out to Destroy … Iran's Bushehr Nuclear Plant?," *Christian Science Monitor*, September 21, 2010; Jonathan Fildes, "Stuxnet Worm Targeted High-Value Iranian Assets," *BBC News*, September 23, 2010; Josh Halliday, "Stuxnet Worm Is the Work of a National Government Agency," *Guardian* (UK), September 24, 2010. For comprehensive accounts of the creation, deployment, and operation of Stuxnet, see David E. Sanger, *Confront and Conceal: Obama's Secret Wars and*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Surprising Use of American Power (New York: Crown, 2012) and Symantec, *W32.Stuxnet Dossier*, version 1.4, February 2011.

222. Symantec, *W32.Stuxnet Dossier*; Carey Nachenberg, "A Forensic Dissection of Stuxnet," Center for International Security and Cooperation, Stanford University, April 23, 2012; Riva Richmond, "Malicious Software Program Attacks Industry," *New York Times*, September 25, 2010.

223. Stuxnet targeted linked elements of the industrial control system. Specifically, it targeted Siemens' SIMATIC WinCC and Step 7 PLCs. Eric Byres, Andrew Ginter, and Joel Langill, "How Stuxnet Spreads," version 1, *Tofino Security White Paper*, February 22, 2011.

224. Sanger, *Confront and Conceal*; Symantec, *W32.Stuxnet Dossier*, Nachenberg, "Forensic Dissection of Stuxnet."

225. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012.

226. Clayton, "Stuxnet Malware Is 'Weapon' Out to Destroy"; Reuters, "UPDATE 2: Cyber Attack Appears to Target Iran-Tech Firms," *Reuters*, September 24, 2010; John Markoff, "A Silent Attack, but Not a Subtle One," *New York Times*, September 26, 2010; Richard A. Falkenrath, "From Bullets to Megabytes," *New York Times*, January 27, 2011; Holger Stark, "Stuxnet Virus Opens New Era of Cyber War," *Spiegel Online*, August 8, 2011.

227. For accounts that discuss infrastructure vulnerability as alternately the product of technological progress, economic laws, or the side effects of neglect, see U.S. Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC, 2002), https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf; Lewis, *Critical Infrastructure Protection*; Stephen Flynn, *The Edge of Disaster: Rebuilding a Resilient Nation* (New York: Random House, 2007).

228. This figure is regularly promoted but it should not be taken to have any serious precision or rigor. See U.S. Office of Homeland Security, *National Strategy*, 73; Tom Ridge, "Remarks by Secretary Tom Ridge to National League of Cities," March 10, 2003, transcript (Washington, DC: Department of Homeland Security), https://www.hsdl.org/?abstract&did=475516.

229. It is worth noting that ostensibly free markets are an active political creation, rather than a "natural" state of affairs outside of political and social life. See Karl Polanyi, *The Great Transformation* (Boston: Beacon Press, 1944).

Chapter 3

1. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC, 1997), 13.

2. POD, "Report of the Superintendent of Railway Mail Service," in *Annual Report of the Post-Master General of the United States for the Fiscal Year Ended June 30, 1878* (Washington, DC: Government Printing Office, 1878), 238.

3. Ibid., 239

4. Ibid., 238–239.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

5. Ryan Ellis, "Disinfecting the Mail: Disease, Panic, and the Post Office Department in Nineteenth-Century America," *Information & Culture: A Journal of History* 52, no. 4 (2017): 436–461.

6. Ibid.

7. Ibid.

8. Mark Aldrich, *Death Rode the Rails: American Railroad Accidents and Safety, 1828–1965* (Baltimore: Johns Hopkins University Press, 2006).

9. Ibid.

10. Ibid., 3.

11. On the thematic continuity and continued salience of terrorism across the administrations of President George W. Bush and President Barack Obama, see Savage, *Power Wars*; Goldsmith, *Power and Constraint*.

12. George W. Bush, "Address to the Nation on the Terrorist Attacks," transcript, The American Presidency Project, September 11, 2001, http://www.presidency.ucsb.edu/ws/?pid=58057.

13. National Commission of Terrorist Attacks Upon the United States, "Executive Summary," in *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2004), http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

14. Exec. Order No. 13228, 66 Fed. Reg. 51812 (Oct. 10, 2001).

15. George W. Bush, "Remarks at the Swearing-In Ceremony for Tom Ridge as Director of the Office of Homeland Security," transcript, The American Presidency Project, October 8, 2001, http://www.presidency.ucsb.edu/ws/?pid=62592.

16. Ibid. (emphasis added).

17. Ibid.

18. Exec. Order No. 13228, 66 Fed. Reg. at 51812.

19. Ibid., at 51813.

20. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107–156, 115 Stat. 272 (2001).

21. Ibid.

22. Ibid.

23. Ibid., § 1016(E).

24. Ibid., § 1016(C)(1).

25. On the coproduction of risk and vulnerability, see Wiebe Bijker, Anique Hommels, and Jessica Mesman, "Studying Vulnerability in Technological Cultures," in *Vulnerability in Technological Cultures: New Directions in Research and Governance*, ed. Anique Hommels, Jessica Mesman, and Wiebe E. Bijker (Cambridge, MA: MIT Press, 2014), 1–26; Sheila Jasanoff, "Vulnerability and Development—Bhopal's Lasting Legacy," in Hommels, Mesman, and Bijker, *Vulnerability in Technological Cultures*, 89–108.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

26. See Andrew Lakoff, "Preparing for the Next Emergency," *Public Culture* 19, no. 2 (2007): 247–271; Stephen Collier and Andrew Lakoff, "The Vulnerability of Vital Systems: How Critical Infrastructure Became a Security Problem," in *The Politics of Securing the Homeland: Critical Infrastructure, Risk and (In) Security*, ed. Myriam Dunn and Kristian Søby Kristensen (London: Routledge, 2008) 17–39; Andrew Lakoff and Eric Klinenberg, "Of Risk and Pork: Urban Security and the Politics of Objectivity," *Theory and Society* 39, no. 5 (2010): 503–525.

27. On the scale of the reorganization that DHS entailed and historical comparisons, see Cuéllar, *Governing Security,* 127.

28. Kathi Ann Brown offers a detailed history of the political consideration of critical infrastructure security in the U.S. during the 20th century. Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States* (Fairfax, VA: Spectrum, 2006). See also Collier and Lakoff, "Vulnerability of Vital Systems."

29. Brown, *Critical Path*, 13–42; Collier and Lakoff, "Vulnerability of Vital Systems."

30. Lakoff, "Preparing," 257.

31. Ibid.

32. Brown, *Critical Path*, 52.

33. Ibid.

34. Ibid., 34.

35. Ibid.

36. Ibid., 52; Richard Nixon, "Memorandum Establishing a Cabinet Committee to Combat Terrorism," September 25, 1972, The American Presidency Project, http://www.presidency.ucsb.edu/ws/?pid=3596; Clinton Granger, "Mass Destruction Terrorism Crisis Management Study (Status Report No. 2)," memorandum for General Scowcroft, National Security Council, June 25, 1975, https://www.cia.gov/library/readingroom/docs/LOC-HAK-74-2-17-9.pdf.

37. Brown, *Critical Path*, 53.

38. Richard H. Wilcox and Patrick J. Garrity, eds., *A Nation of Vulnerabilities: Crisis Management in a Society of Networks* (Washington DC: Center for Strategic and International Studies, Georgetown University, 1984). See also Brown, *Critical Path*, 53.

39. Wilcox and Garrity, *Nation of Vulnerabilities*.

40. Ibid., 6.

41. Ibid., 4–5.

42. William J. Clinton, "Presidential Decision Directive 39—U.S. Policy on Counterterrorism," Federation of American Scientists, June 21, 1995, https://fas.org/irp/offdocs/pdd39.htm; Brown, *Critical Path*, 72.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

43. Clinton, "Presidential Decision Directive 39."
44. Ibid.
45. Brown, *Critical Path*, 74.
46. Ibid., 74–80.
47. Ibid.
48. Exec. Order No. 13010, 61 Fed. Reg. 37347 (July 17, 1996).
49. Ibid.
50. President's Commission on Critical Infrastructure Protection, *Critical Foundations*, iii.
51. Ibid., 7–8.
52. Ibid., 4–6.
53. Ibid., 5.
54. Ibid., 8.
55. Ibid., 8.
56. Ibid., 10, A-11, A-38, A-48.
57. Ibid., 10.
58. Ibid., 25–100.
59. Quoted in Brown, *Critical Path*, 137.
60. Ibid., 139.
61. Ibid., 138.
62. Ibid., 139.
63. "President Bill Clinton Speaks to the Naval Academy at Annapolis," transcript, CNN.com, May 22, 1998, http://www.cnn.com/ALLPOLITICS/1998/05/22/clinton.academy/transcript.html.
64. Quoted in Brown, *Critical Path*, 139.
65. William J. Clinton, "Presidential Decision Directive/NSC 63—Critical Infrastructure Protection," Federation of American Scientists, May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.
66. Ibid.
67. Ibid.
68. Ibid.
69. Ibid.
70. Ibid.
71. Ibid.
72. GAO, *Critical Infrastructure Protection: Federal Efforts*, 27.
73. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, 32.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

74. U.S. Commission on National Security/21st Century, *Road Map for National Security: Imperative for Change*, phase III report of the U.S. Commission on National Security/21st Century (Washington, DC, 2001).

75. Ibid., vii.

76. See John D. Moteff, *Critical Infrastructures: Background and Early Implementation of PDD-63*, prepared by the Congressional Research Service (Washington, DC: Library of Congress, 2001), 15.

77. Aspen Institute Justice and Society Program and the Annenberg Public Policy Center of the University of Pennsylvania, *Alarms Unheeded: Lessons on the 13th Anniversary of the Final Hart-Rudman Report*, 2014, 10, https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/Alarms-Unheeded.pdf.

78. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, 8–11.

79. Cuéllar, *Governing Security*, 136.

80. Ibid., 125–137.

81. Ibid., 137.

82. See ibid., 125–150.

83. Ibid., 139.

84. Ibid., 139.

85. Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (2002).

86. George W. Bush, "Remarks by the President at the Signing of H.R. 5005 the Homeland Security Act of 2002," November 25, 2002, transcript, The White House, President George W. Bush (italics added), https://georgewbush-whitehouse.archives.gov/news/releases/2002/11/20021125-6.html.

87. Ibid.; Cuéllar, *Governing Security*, 137–150.

88. Cuéllar, *Governing Security*, 146.

89. Homeland Security Act.

90. Ibid., § 101(b).

91. Ibid., § 201(a)(b).

92. Ibid., § 201(d).

93. Ibid.

94. U.S. Department of Homeland Security, *Budget in Brief: Fiscal Year 2005* (Washington, DC, 2005), https://www.dhs.gov/sites/default/files/publications/FY_2005_BIB_4.pdf, 13.

95. DHS has undergone multiple internal reorganizations. The Directorate of Information Analysis and Infrastructure Protection was renamed the Directorate for Preparedness. Later, the Directorate for Preparedness was renamed the National Protection and Programs Directorate. Through these changes the directorate retained its existing mission, and the position of assistant secretary for Infrastructure Protection remained in place. See Stephen R. Vina, *Homeland*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Security: Scope of the Secretary's Reorganization Authority, prepared by the Congressional Research Service (Washington, DC: Library of Congress, 2005), 5, https://fas.org/sgp/crs/homesec/RS21450.pdf; Harold C. Relyea and Henry B. Hogue, *Department of Homeland Security Reorganization: The 2SR Initiative*, prepared by the Congressional Research Service (Washington, DC: Library of Congress, 2006), https://www.hsdl.org/?view&did=467158; Elizabeth C. Borja, *Brief Documentary History of the Department of Homeland Security: 2001–2008* (Washington, DC: Department of Homeland Security, 2008), https://www.hsdl.org/?view&did=37027.

96. Figures tabulated OMB, "Appendix: Homeland Security."

97. Ibid.

98. This figure excludes funds marked for border and transportation security. If they are added into the mix, the total funding climbs to over $51 billion and 70% of total homeland security funding. Ibid.

99. See Cuéllar, *Governing Security*, 127.

100. Ibid.

101. Quoted in Brown, *Critical Path*, 140.

102. Ryan Ellis, "Appropriating Risk: National Security and the Sunrise Powerlink Controversy" (paper presented at the National Communication Association Annual Convention, San Francisco, November 2011).

103. On crises and control, see James Beniger, *The Control Revolution: Technological and Economic Origins of Information Society* (Cambridge, MA: Harvard University Press, 1986).

104. Ulrich Beck, "The Reinvention of Politics," in *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*, ed. Ulrich Beck, Anthony Giddens, and Scott Lash (Stanford, CA: Stanford University Press, 1994), 6.

105. Quoted in Deborah Lupton, *Risk* (New York: Routledge, 1999), 74. See Anthony Giddens, "Living in a Post-traditional Society," in Beck, Giddens, and Lash, *Reflexive Modernization*, 56–109.

106. Beck, *Risk Society*, 19.

107. Beck's thesis concerning risk society is developed in numerous texts; see Beck, *Risk Society*, 1–50; Beck, *World at Risk*; Ulrich Beck, "Global Risk Politics," *Political Quarterly* 68 (1997): 18–33; Beck, "Reinvention of Politics." For useful commentary, see Scott Lash and Brian Wynne, "Introduction" in Beck, *Risk Society*, 1–8; Lupton, *Risk*; Beck, Giddens, and Lash, *Reflexive Modernization*.

108. Beck, *Risk Society*, 20–21.

109. Beck, *Risk Society*, 19–50; Beck, "Global Risk Politics"; Beck, *World at Risk*, 47–66.

110. Beck, "Global Risk Politics," 25–26; Beck, *Risk Society*, 22–34; Beck, *World at Risk*, 47–66; Lupton, *Risk*, 64–65.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

111. In this manner, *risks*, as Beck sketches the term, appear to be what are often described within the literature on risk as *uncertainties*. The classic distinction between risk, for which probabilistic estimates can be made, and uncertainty, for which such estimates cannot, is found in Knight, *Risk, Uncertainty, and Profit* (1921; repr., 1957). Beck's notion of risks is more closely aligned with what Knight terms uncertainty. Indeed, Beck adopts the phrase *manufactured uncertainties* in discussing the types of novel risks in which he is interested. Beck, *World at Risk*, 50. For a discussion of the disjunction between Beck's use of the term *risk* and its usage within economics and the literature on risk analysis, see Lupton, *Risk*, 7–8.

112. On this point, see also Francois Ewald, "Insurance and Risk," in *The Foucault Effect: Studies of Governmentality*, ed. Graham Burchell, Colin Gordon, and Peter Miller (Chicago: University of Chicago Press, 1991), 197–210.

113. Beck, *Risk Society*; Beck, *World at Risk*; Beck, "Global Risk Politics"; Beck, "Reinvention of Politics." On the conceptual and policy challenges and difficulties of addressing what are often termed low-probability, high-consequence events, see Richard Posner, *Catastrophe: Risk and Response* (New York: Oxford University Press, 2005); Philip Auerswald et al., eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerabilities* (Cambridge: Cambridge University Press, 2006); Cass Sunstein, *Worst-Case Scenarios* (Cambridge, MA: Harvard University Press, 2007).

114. See Beck, "Reinvention of Politics," 18; Beck, "Global Risk Politics," 29–30; Beck, *Risk Society*, 28–47; Beck, *World at Risk*, 21.

115. Beck, *Risk Society*, 77.

116. Ibid.

117. In this sense, risks operate as what political scientists describe as *policy windows*. See Thomas A. Birkland, *After-Disaster: Agenda Setting, Public Policy, and Focusing Events* (Washington, DC: Georgetown University Press, 1997); Thomas A. Birkland, *Lessons of Disaster: Policy Change after Catastrophic Events* (Washington, DC: Georgetown University Press, 2006).

118. Beck, "Global Risk Politics," 32.

119. Beck, Giddens, and Lash, *Reflexive Modernization*, vii; Beck, *World at Risk*, 30, 68–69, 135.

120. For a discussion of how social movements can appropriate risk, see Kim Fortun, *Advocacy after Bhopal: Environmentalism, Disaster, New Global Orders* (Chicago: University of Chicago Press, 2001).

121. Beck, "Reinvention of Politics," 29; Ulrich Beck, "Self-Dissolution and Self-Endangerment of Industrial Society: What Does This Mean?," in *Reflexive Modernization*, 178.

122. Ulrich Beck, Wolfgang Bonns, and Christoph Lau, "The Theory of Reflexive Modernization," *Theory, Culture & Society* 20, no. 2 (2016): 20.

123. Beck, *Risk Society*, 29.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

124. Ibid., 47–48.

125. Beck, *World at Risk*, 66.

126. Ibid., 30–34.

127. Ibid., 21.

128. Beck, *Risk Society*, 49–50; Beck, "Self-Dissolution," 177; Beck, *World at Risk*, 57–59.

129. Beck, *Risk Society*, 78–81.

130. Beck, *World at Risk*, 32.

131. Beck's discussion of the staging of risks in *World at Risk* highlights that collective knowledge and recognition of a risk is indispensable to its utility as a resource (10–16). See also Beck, *Risk Society*, 33–34.

132. Geertz's notion of culture is informed most significantly by the work of Max Weber. See Clifford Geertz, "Thick Description: Toward an Interpretive Theory of Culture," in *The Interpretation of Cultures: Selected Essays* (New York: Basic, 1973), 3–30.

133. Beck, *World at Risk*, 66.

134. Beck, "Global Risk Politics," 30.

135. See Ann Swidler, "Culture in Action: Symbols and Strategies," *American Sociology Review* 51 (1986): 273–286.

136. Barry Buzan, Ole Weaver, and Jaap De Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner, 1998).

137. Ibid., 23.

138. Ibid., 29.

139. Corey Robin, *Fear: History of a Political Idea* (New York: Oxford University Press, 2004).

140. Robin's discussion and use of *fear* is analogous to Beck's more colloquial use of risks to mean perception of harm or danger.

141. John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (New York: Free Press, 2006). The argument that risks are used to justify the extension of power is also evident in the work of Robert Higgs and Naomi Klein. Higgs sees the appropriation of risks as driving the growth of the powerful administrative state, while Klein sees the same process as fostering the evisceration of public controls designed to protect public welfare in favor of powerful corporate interests. See Robert Higgs, *Crisis and Leviathan: Critical Episodes in the Growth of American Government* (New York: Oxford University Press, 1987); Klein, *Shock Doctrine*.

142. James Carey, "A Cultural Approach to Communication," in *Communication as Culture: Essays on Media and Society* (New York: Routledge, 1992), 13–36.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Chapter 4

An earlier version of this chapter appeared as Ryan Ellis, "Creating a Secure Network: The 2001 Anthrax Attacks and the Transformation of Postal Security," supplement, *Sociological Review* 62 (1 suppl) (2014): 161–182.

1. Quoted in Pam Belluck, "Post Office Handles Less Mail, With More Caution," *New York Times*, October 21, 2001.

2. Anthrax is the disease caused by spores of the bacterium *Bacillus anthracis*. Infection can take three different forms: inhalation, cutaneous, and gastrointestinal. As is colloquial, *anthrax* will be used to refer to both the spores of *Bacillus anthracis* and the disease that can result from exposure. It is presumed that not all of the letters initially treated with anthrax were recovered. See Thomas V. Inglesby et al., "Anthrax as a Biological Weapon, 2002: Updated Recommendations for Management," *Journal of the American Medical Association* 287, no. 17 (2002): 2237; Affidavit of Thomas F. Dellafera in Support of Search Warrant, No. 07–524-M-01 (D.D.C. 2007); Thomas V. Inglesby et al., "Anthrax as a Biological Weapon: Medical and Public Health Management," *Journal of the American Medical Association* 281, no. 18 (1999): 1735–1745.

3. See Inglesby et al., "Anthrax as a Biological Weapon, 2002"; Affidavit of Thomas F. Dellafera; Inglesby et al., "Anthrax as a Biological Weapon."

4. See Committee on Standards and Policies for Decontaminating Public Facilities Affected by Exposure to Harmful Biological Agents: How Clean Is Safe?, *Reopening Public Facilities after a Biological Attack: A Decision Making Framework* (Washington, DC: National Academies Press, 2005), 1–22.

5. Nye Stevens, *Postal Service Financial Problems and Stakeholder Proposals*, prepared by the Congressional Research Service, RL31069 (Washington, DC: Library of Congress, 2002); Frank Gottron, *The U.S. Postal Service Response to the Threat of Bioterrorism through the Mail*, prepared by the Congressional Research Service, RL31280 (Washington, DC: Library of Congress, 2009); *Financial Security of the US Postal Service: Hearing before a Subcomm. of the Comm. on Appropriations*, 107th Cong. 284 (2001) (statement of John E. Potter, Postmaster General/CEO), https://www.gpo.gov/fdsys/pkg/CHRG-107shrg77771/pdf/CHRG-107shrg77771.pdf; Committee on Decontaminating Public Facilities, *Reopening Public Facilities*, 1.

6. U.S. Postal Inspection Service, *2002 Annual Report of Investigations of the United States Postal Inspection Service* (Washington, DC, 2002), 12, https://postalinspectors.uspis.gov/pressroom/pubs.aspx.

7. Lee Heath, "Weapons of Mass Disruption" (presentation to Mailers' Technical Advisory Committee, Washington, DC, May 7, 2003), https://ribbs.usps.gov/mtac/documents/tech_guides/.

8. The investigation into the anthrax mailings eventually identified a U.S. biodefense researcher as the likely source. On the initial response of policy-makers, see Richard Rhodes, *The Twilight of the Bombs: Recent Challenges, New Dangers, and the Prospect for a World without Nuclear Weapons* (New York: Knopf, 2010).

9. Star, "Ethnography of Infrastructure."

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

10. Theodore J. Cieslak and Edward M. Eitzen, "Clinical and Epidemiological Principles of Anthrax," *Emerging Infectious Diseases* 5, no. 4 (1999): 552. See also Donald Henderson, "The Looming Threat of Bioterrorism," *Science* 283, no. 5406 (1999): 1279–1282; Inglesby et al., "Anthrax as a Biological Weapon," 1735–1745; Tom Mangold and Jeff Goldberg, *Plague Wars: A True Story of Biological Warfare* (New York: St. Martin's, 2000).

11. Gisa Weszkalnys, "Anticipating Oil: The Temporal Politics of a Disaster Yet to Come," supplement, *Sociological Review* 62, no. S1 (2014): 211–235.

12. Thomas V. Inglesby, "Anthrax: A Possible Case History," *Emerging Infectious Diseases* 5, no. 4 (1999): 556.

13. See James C. Pile et al., "Anthrax as a Potential Biowarfare Agent," *Archive of Internal Medicine* 158, no. 5 (1998): 429–434; Inglesby et al., "Anthrax as a Biological Weapon, 2002," 2236–2252; World Health Organization, *Health Aspects of Chemical and Biological Weapons* (Geneva: World Health Organization, 1970), 84–100; Elizabeth Fee and Theodore M. Brown, "Preemptive Biopreparedness: Can We Learn Anything from History?," *American Journal of Public Health* 91, no. 5 (2001): 721–726.

14. OTA, *Proliferation of Weapons of Mass Destruction: Assessing the Risk*, OTA-ISC-559 (Washington, DC: Government Printing Office, 1993); Henderson, "Looming Threat of Bioterrorism," 1279–1282.

15. Centers for Disease Control and Prevention, "Bioterrorism Alleging Use of Anthrax and Interim Guidelines for Management—United States, 1998," *MMWR Weekly* 48, no. 4 (1999): 69–74; B. Kournikakis et al., *Risk Assessment of Anthrax Threat Letters*, DRES TR-2001–048 (Suffield, Alberta: Defence Research Establishment Suffield, 2001), 1.

16. Elizabeth Etheridge, *Sentinel for Health: A History of the Centers for Disease Control* (Berkeley: University of California Press, 1992); Fee and Brown, "Preemptive Biopreparedness," 721–726; Russ Zajtchuk and David Franz, "Biological Terrorism," in *Terrorism: Reducing Vulnerabilities and Improving Responses*, by Committee on Counterterrorism Challenges for Russia and the United States (Washington, DC: National Academies Press, 2004), 214–221.

17. See GAO, *Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives*, GAO/T-NSIAD-99–112 (Washington, DC, 1999); GAO, *Combating Terrorism: Linking Threats to Strategies and Resources*, GAO/T-NSIAD-00–218 (Washington, DC, 2000); Etheridge, *Sentinel for Health*, 42–47.

18. Centers for Disease Control and Prevention, "Bioterrorism Alleging Use of Anthrax."

19. USPS, "Emergency Response to Mail Allegedly Containing Anthrax," Management Instruction EL-860-1999-3, Washington, DC, October 4, 1999.

20. Ibid.

21. The letters sent to NBC, the *New York Post*, and both senators were recovered. Investigators established the presence of additional letters based on

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

environmental testing and additional evidence, though not all presumed letters were recovered. Affidavit of Thomas F. Dellafera; GAO, *US Postal Service: Better Guidance Needed to Ensure Appropriate Response to Anthrax Contamination*, GAO-04–239 (Washington, DC, 2004), 12.

22. GAO, *Bioterrorism: Public Health Response to Anthrax Incidents of 2001*, GAO-04–152 (Washington, DC, 2003), 9.

23. GAO, *Automation Is Taking Longer*.

24. GAO, *Bioterrorism*.

25. Center for Counterproliferation Research, "Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks" (working paper, Center for Counterproliferation Research, National Defense University, Washington, DC, 2002), 73, http://www.fas.org/irp/threat/cbw/anthrax.pdf.

26. Quoted in Center for Counterproliferation Research, "Anthrax in America."

27. See T. W. Luke, "Everyday Techniques as Extraordinary Threats: Urban Technostructures and Non-places in Terrorist Actions," in *Cities, War, and Terrorism*, ed. Stephen Graham, 120–136.

28. See Beck, *Risk Society*; Beck, *World at Risk*.

29. Canadian defense researchers conducted the only known laboratory tests of the distribution of anthrax through the mail prior to the fall of 2001 and echoed the conclusions reached by the CDC and USPS. See Kournikakis et al., "Risk Assessment," 13.

30. Quoted in Center for Counterproliferation Research, "Anthrax in America," 45.

31. See Centers for Disease Control and Prevention, "Bioterrorism Alleging Use of Anthrax"; USPS, "Emergency Response to Mail Allegedly Containing Anthrax."

32. It is likely that testing did not identify the full scope of cross-contamination. For a discussion of the limitations of the testing process, see GAO, *Anthrax Detection: Agencies Need to Validate Sampling Activities in Order to Increase Confidence in Negative Results*, GAO-05–251 (Washington, DC, 2005).

33. American Postal Workers Union, "Oct. 25 Teleconference a Success," October 26, 2001, accessed November 1, 2008, http://www.apwu.org/news/burrus/2001/update57-2001-102601.htm; American Postal Workers Union, "Steps to Insure Protection from Anthrax," November 8, 2001, accessed March 8, 2014, http://www.apwu.org/news/burrus/2001/update58-2001-110801.htm; American Postal Workers Union, "Anthrax-Contaminated Facilities Must Be Decontaminated and Tested," November 19, 2001, accessed March 8, 2014, http://www.apwu.org/news/burrus/2001/update59-2001-111901.htm; Jessica Reaves, "The Anthrax Saga Continues," *Time*, November 2, 2001; USPS Office of Inspector General (OIG), "Fact-Finding Review of Actions and Decisions by Postal Service Management at the South Jersey Processing and Distribution Center," LH-MA-02–004 (Bellmawr, NJ, 2002).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

34. American Postal Workers Union, "Union, Management Reach Fork in the Road on Anthrax Policy," November 21, 2001, accessed March 8, 2014, http://www.apwu.org/news/nsb/2001/nsb31-2001-112701.htm.

35. Quoted in Robert Finn, "Union Chief's Battle Is with the Postal Service," *New York Times*, November 1, 2001.

36. Andrew Lakoff, "From Population to Vital System: National Security and the Changing Object of Public Health," in *Biosecurity Interventions: Global Health and Security in Question*, ed. Andrew Lakoff and Stephen Collier (New York: Columbia University Press, 2008), 33–60.

37. Ibid.

38. Larry Riggs, "Lettershops Brace for Slowdown," *Direct*, October 18, 2001; Patricia Odell, "Live from Chicago: Wientzen, A Tumultuous Year for DMers," *Direct*, October 29, 2001; Beth Negus Viveiros, "NEDMA Holds Town Meeting to Discuss Anthrax Crisis," *Direct*, November 2, 2001.

39. Ray Schultz, "Direct Hit: Mail War," *Direct*, October 16, 2001; Riggs, "Lettershops Brace for Slowdown"; Kris Oser, "Boardroom Braces for Anthrax Fallout," *Direct*, October 24, 2001; "Reader's Digest Hurt by 9/11 and Anthrax Scare," *Direct*, January 24, 2002.

40. GAO, *Primer on Postal Worksharing*.

41. GAO, *Highlights of GAO's Conference on Options to Enhance Mail Security and Postal Operations*, GAO-02-315SP (Washington, DC, 2001); Jim Rowan, "Mail Security Task Force Update" (presentation to Mailers' Technical Advisory Committee, Washington, DC, February 2002).

42. Ibid.

43. USPS, "Postmaster General Announces Mail Security Task Force," press release no. 01–089, October 15, 2001, Avalon Project, Yale Law School, http://avalon.law.yale.edu/sept11/usps_002.asp.

44. American Postal Workers Union, "Federal Judge Dismisses APWU Lawsuit against Bush," December 4, 2008, accessed June 19, 2012, http://www.apwu.org/news/webart/2008/08118-bushlawsuit-081204.htm; Mailers' Technical Advisory Committee, *MTAC Charter* (Washington, DC: USPS, 2013), http://ribbs.usps.gov/mtac/documents/tech_guides/mtac_charter.pdf.

45. See Beck, *Risk Society*; Beck, *World at Risk*.

46. GAO, *Highlights*; USPS, *Emergency Preparedness Plan*.

47. Tom Day, "Mail Sanitization Update" (presentation to Mailers' Technical Advisory Committee, Washington, DC, February 2002), https://ribbs.usps.gov/mtac/documents/tech_guides/.

48. Gary Green et al., *Investigation of the Health Effects of Irradiated Mail*, report of the General Counsel of the Office of Compliance, U.S. Congress, OSH-0201,0202 (Washington, DC, 2002).

49. USPS OIG, *Audit Report—Postal Service Strategy for Processing At-Risk Mail and Deployment of Irradiation Equipment*, AC-AR-02-003 (Washington, DC, 2002).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

50. GAO, *United States Postal Service: Information on the Irradiation of Federal Mail in the Washington, DC, Area*, briefing to the House and Senate Appropriations Committees, GAO-08-938R (Washington, DC, 2008).

51. Tom Day, "Mail Sanitization" (presentation to Mailers' Technical Advisory Committee, Washington, DC, November 8, 2001), https://ribbs.usps.gov/mtac/documents/tech_guides/.

52. Gottron, *Threat of Bioterrorism*.

53. Rowan, "Mail Security Task Force," February 2002.

54. Green et al., *Health Effects of Irradiated Mail*; National Institute for Occupational Safety and Health, *NIOSH Health Hazard Evaluation Report: HETA #2002-0136-2880, United States Senate and House of Representatives, Washington, DC* (Cincinnati: Department of Health and Human Services, 2002).

55. USPS OIG, *Deployment of Irradiation Equipment*.

56. Select federal mail remains subject to irradiation.

57. *Stamping Out Anthrax in USPS Facilities: Technologies and Protocols for Bioagent Detection, Hearing Before the Subcomm. on National Security, Emerging Threats and International Relations*, 108th Cong. (2003) (statement of William Burrus, President, American Postal Workers Union).

58. USPS Engineering, "Decision Analysis Report: Biohazard Detection Systems" (Washington, DC, 2004); USPS OIG, *Audit Report—Biohazard Detection System Consumables*, DA-AR-06–006 (Washington, DC, 2006).

59. See USPS, *2005 Comprehensive Statement on Postal Operations* (Washington, DC, 2005); USPS, *2006 Comprehensive Statement on Postal Operations* (Washington, DC, 2006); USPS OIG, *Postal Service's Efforts to Implement Prevention and Detection Technology*, DA-AR-02–008 (Washington, DC, 2002); USPS OIG, *Biohazard Detection System Consumables*.

60. Rowan, "Mail Security Task Force," February 2002; USPS OIG, *Effort to Implement*; USPS OIG, *Biohazard Detection System*, DA-MA-02-001 (Washington, DC, 2002).

61. USPS, "FAQ: What Is the USPS Biohazard Detection System?," n.d., https://about.usps.com/news/state-releases/sc/2013/FAQ-BDS.pdf.

62. See USPS, *Emergency Preparedness Plan*; USPS OIG, *Biohazard Detection System*.

63. On DBCS and reaerosolization, see Peter M. Dull et al., "*Bacillus anthracis* Aerosolization Associated with a Contaminated Mail Sorting Machine," *Emerging Infectious Diseases* 8, no. 10 (2002): 1044–1047; Eyasu H. Teshale et al., "Environmental Sampling for Spores of *Bacillus anthracis*," *Emerging Infectious Diseases* 8, no. 10 (2002): 1083–1087; Puneet K. Dewan et al., "Inhalational Anthrax Outbreak among Postal Workers, Washington, DC, 2001," *Emerging Infectious Diseases* 8, no. 10 (2002): 1066–1072.

64. See Leonard A. Cole, *The Anthrax Letters: A Medical Detective Story* (Washington, DC: John Henry Press, 2003).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

65. USPS, "Decision Analysis Report"; USPS, *Update on Biohazard Detection System in Response to OIG Report #DA-MA-02–001* (Washington, DC, 2004).

66. See Paul M. Alberta, "USPS Expected to Seek as Much as $10 Billion in Aid from Congress," *Direct*, November 7, 2001; GAO, *Highlights*; Rowan, "Mail Security Task Force," February 2002.

67. See Spencer S. Hsu, "Anthrax Alarm Uncovers Response Flaws," *Washington Post*, March 17, 2005; USPS OIG, *Biohazard Detection System Consumables*; Elizabeth Lester, Gregory Bearman, and Adrian Ponce, "A Second Generation Anthrax Smoke Detector: An Inexpensive Front-End Monitor That Detects Bacterial Spores," *IEEE Engineering in Medicine and Biology* 23, no. 1 (2004): 130–135.

68. Based on available USPS cost data and OIG audits, it appears that appropriated federal funds have paid for less than half of the costs of the BDS. See USPS, *Emergency Preparedness Plan*, 6–5; USPS, *Update on Biohazard Detection System*, 5; USPS, *Response to the House Subcommittee on Transportation, Treasury, Housing and Urban Development, the Judiciary, District of Columbia and the Senate Subcommittee on Transportation, Treasury, Judiciary, Housing and Urban Development, Committees on Appropriations* (Washington, DC, 2006); USPS, *2006 Comprehensive Statement*, 61; USPS OIG, *Effort to Implement*; USPS OIG, *Biohazard Detection System Consumables*.

69. USPS, "FAQs about Security Controls for Commercial Mailers," https://about.usps.com/securing-the-mail/controls-for-commercial-mailers-faqs.htm, accessed September 29, 2017; Jim Rowan, "Mail Security Task Force Update" (presentation to Mailers' Technical Advisory Committee, Washington, DC, May 2002).

70. USPS OIG, *Biohazard Detection System*.

71. *Stamping Out Anthrax in USPS Facilities: Technologies and Protocols for Bioagent Detection, Hearing Before the Subcomm. on National Security, Emerging Threats and International Relations*, 108th Cong. (2003) (statement of William Burrus, President, American Postal Workers Union).

72. GAO, *Primer on Postal Worksharing*.

73. See Lyon, *Surveillance after September 11*.

74. Intelligent Document Task Force, *Pursuing the Intelligent Document: A Vision for Paper-Based Communications in the Information Age: Phase I Report* (Washington, DC: USPS, 1999); Intelligent Document Task Force, *Pursuing the Intelligent Document: A Review of Technologies Impacting the Future of Mail, Phase II Report* (Washington, DC: USPS, 2001); Intelligent Document Task Force, *The Internet of Things: The Final Report of the Intelligent Document Task Force* (Washington, DC: USPS, 2004); Mailing Industry Task Force, *Seizing Opportunity: The 2001 Report of the Mailing Industry Task Force* (Washington, DC: USPS, 2001).

75. See Pam Gibert, "Using Intelligent Technology for Mail Security" (presentation to Mailers' Technical Advisory Committee, Washington, DC, November 8, 2001), https://ribbs.usps.gov/mtac/documents/tech_guides/; Intelligent

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Document Task Force, *Pursing the Intelligent Document*; Mailing Industry Task Force, *Promote Development of Intelligent Mail* (Washington, DC: USPS, 2003).

76. GAO, *US Postal Service: Intelligent Mail Benefits May Not Be Achieved if Key Risks Are Not Addressed*, GAO-09–599 (Washington, DC, 2009), 28.

77. USPS, *Intelligent Mail Vision: Rev. 2.0 for RIBBS*, accessed July 2009; site now discontinued, https://ribbs.usps.gov/intelligentmail_latestnews/documents/tech_guides/IMVision2009.pdf, 4.

78. Ibid., 25–29.

79. USPS Delivery Support Headquarters, *How to Succeed with MSP* (Washington, DC: USPS, 2002), 29.

80. Mailing Industry Task Force, *Seizing Opportunity*.

81. USPS, "Intelligent Mail Vision."

82. See Stephen Graham and Simon Marvin, *Splintering Urbanism: Networked Infrastructures, Technological Motilities, and the Urban Condition* (New York: Routledge, 2001).

83. Intelligent Document Task Force, *Pursuing the Intelligent Document*; USPS, *United States Postal Service Transformation Plan*.

84. Mailing Industry Task Force, *Seizing Opportunity*, 19.

85. Since the mid-1980s, the growth of casual workers has outpaced the growth of career employees. From 1987 to 2007, total career employees declined by 8.8%, while noncareer employees increased by 106.5%. Wendy Ginsberg, *US Postal Service Workforce Size and Employment Categories, 1987–2007*, prepared by the Congressional Research Service, RS22864 (Washington, DC: Library of Congress, 2008), 1–5.

86. USPS, *Intelligent Mail Vision*, 9–33.

87. Gibert, "Using Intelligent Technology"; Mailing Industry Task Force, *Promote Development*.

88. USPS, *Emergency Preparedness Plan*.

89. GAO, *Highlights*; Gibert, "Using Intelligent Technology"; Rowan, "Mail Security Task Force," February 2002.

Chapter 5

1. Quoted in "Biden Introduces Rail Security Legislation in Senate," Brotherhood of Locomotive Engineers and Trainmen, June 16, 2005, accessed September 29, 2017, https://www.ble-t.org/pr/news/pf_newsflash.asp?id=4127.

2. Greenpeace, "Protesters Simulate Fatalities of Chemical Attack in Front of US Capitol," news release, September 13, 2005, http://www.greenpeace.org/usa/news/capitolchemicalattacksimulation/.

3. Association of American Railroads (AAR), "Railroads and Chemicals," May 2019, https://www.aar.org/wp-content/uploads/2018/05/AAR-Railroads-Chemicals.pdf.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

4. Ibid.

5. Ibid.

6. Interim Final Rule: Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments, 73 Fed. Reg. 20752–20773 (April 16, 2008).

7. Jay Boris testimony, quoted in Kathy Patterson, "Councilmember Patterson's Statement on Introduction," January 28, 2005, The Terrorism Prevention in Hazardous Materials Transportation Act of 2005, 53 D.C. Reg. 1047 (April 28, 2006); Ross. C. Paolino, "All Aboard! Making the Case for a Comprehensive Rerouting Policy to Reduce the Vulnerability of Hazardous Railcargoes to Terrorist Attack," *Military Law Review* 193 (2007): 148.

8. "Biden Introduces Rail Security Legislation." See also Esther D'Amico, "Moving through Unfriendly Territory," *Chemical Week*, January 25, 2006.

9. For information on Greenpeace's long-standing campaign against the use of toxic chemicals, particularly chlorine, see Greenpeace International, *Annual Report*, multiple vols. (Amsterdam: Greenpeace International, 1994–2009), http://www.greenpeace.org/international/en/about/reports/.

10. "Hell on Wheels: Why Are Trains That Carry Potentially Lethal Cargo Allowed to Transit the Capital?," editorial, *Washington Post*, March 12, 2006; Greenpeace, "Re-routing Will Eliminate Catastrophic Risks," comment on *Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments*, No. PHMSA-RSPA-2004-18730 (Washington, DC: Pipeline and Hazardous Materials Safety Administration [PHMSA], February 16, 2007).

11. On the issue of rerouting, the rail and chemical industries aligned to reject government intervention. On other key issues, however, the rail and chemical industries sharply disagreed. Railroads supported legislation promoting the adoption of inherently safer technologies and the relaxation of common-carrier obligations that would have allowed them to refuse to carry hazmat cargo. On both these issues, the chemical industry actively challenged the position of the railroads. See *The Rail and Mass Transit Security: Industry and Labor Perspectives, Hearing Before the Subcomm. on Transportation Security and Infrastructure Security*, 110th Cong. (2007) (statement of Nancy Wilson, Vice President for Security, Association of American Railroads); AAR, *Hazmat Transportation by Rail: An Unfair Liability*, Washington, DC, September 2009, http://thehill.com/sites/default/files/aar_hazmatbyrailseptember2009_0.pdf.

12. American Chemistry Council, "Submitted Comments," comment on *Hazardous Materials: Enhancing Rail Transportation Security for Toxic Inhalation Hazard Materials*, No. RSPA-2004-18730 (Washington, DC: Research and Special Programs Administration [RSPA], October 18, 2004); E. I. DuPont de Nemours and Company, "Submitted Comments," comment on *Hazardous Materials*, No. RSPA-2004–18730 (February 14, 2005).

13. Railroads are not only prevented from refusing cargo due to common-carrier obligations but are also limited as to how much they can mark up rates

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

for hazmat cargo. The most obvious ways for the railroads to deal with the challenges of hazmat transportation—refusal to carry and excessive price—are not available. AAR, *Hazmat Transportation*.

14. TIH materials are gases or liquids that are toxic to humans. They are particularly dangerous due to their ability to disperse over large areas. TIH materials, or as they are occasionally dubbed, poisonous-by-inhalation materials, accounted for only .25% of annual railcar loads during the early 2000s. Hazardous materials, in total, during this period accounted for 5.5% of railcar loads. See Request for Comments, Hazardous Materials: Enhancing Rail Transportation Safety and Security for Toxic Inhalation Hazard Materials, 69 Fed. Reg. 50988 (August 16, 2004); AAR, *Hazmat Transportation*.

15. Union Pacific Railroad Company, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (February 20, 2007).

16. "Hazmat FAQ," AAR, accessed November 19, 2010, http://www.aar.org/Safety/Hazmat/Hazmat-FAQ.aspx.

17. *Chemical Attack on America: How Vulnerable Are We? Hearing before the S. Comm. on Homeland Security and Governmental Affairs*, 109th Cong. (2005) (statement of Richard A. Falkenrath, Brookings Institution).

18. Accidents involving hazardous materials were a frequent problem during the 19th and early 20th centuries (see chapter 3). In 1903, an accident involving explosive shipments in the Pennsylvania Railroad yard in Crestline, Ohio, set 500 railcars on fire, injured many, and left a 40 ft. crater in the ground. The Crestline accident provided the impetus for voluntary regulations and the formation of the Bureau of Explosives. Previously, shipments of hazardous materials were governed by private contracts and provisions taken from English common law. An 1866 federal law relating to hazardous cargo was ineffectual and largely ignored. Mark Aldrich, "Regulating Transportation of Hazardous Substances: Railroads and Reform, 1883–1930," *Business History Review* 26, no. 2 (2002): 267–297; OTA, *Transportation of Hazardous Materials*, OTA-SET-304 (Washington, DC: Government Printing Office, 1986), 145–147.

19. Aldrich, "Regulating Transportation," 267–285.

20. Ibid., 267–297; OTA, *Transportation of Hazardous Materials*, 146.

21. Ibid., 146–147.

22. Ibid.; William A. Maurer, "The Transportation of Hazardous Materials after September 11: Issues and Developments," *Federalist Society for Law and Public Policy Studies*, December 1, 2003, https://fedsoc.org/commentary/publications/the-transportation-of-hazardous-materials-after-september-11-issues-and-developments. See Hazardous Materials Transportation Control Act of 1970, Pub. L. No. 91–458 tit. III, 84 Stat. 977 (1970); Hazardous Materials Transportation Act of 1975, Pub. L. No. 93–663, 99 Stat. 2156 (1975). General authority for rail safety in general was granted in the Federal Railroad Safety Act of 1970, Pub. L. No. 91–458 tit. II, 84 Stat. 971 (1970).

23. Over 30,000 different materials are identified within federal hazardous materials regulations. OTA, *Transportation of Hazardous Materials*, 147.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

24. Ibid., 145–185.

25. Ibid., 162.

26. *Reauthorization of the Federal Rail Safety Program: Hearing Before the Subcomm. on Railroads, Pipelines, and Hazardous Materials of the H. Comm. Transportation and Infrastructure*, 110th Cong. 158–193 (2007) (statement of Edward E. Hamberger, President and CEO, AAR); AAR, *Hazmat Transportation*.

27. AAR, *Hazmat Transportation*; Christopher P. L. Barkan, C. Tyler Dick, and Robert Anderson, "Analysis of Railroad Derailment Factors Affecting Hazardous Materials Transportation Risk" (paper presented at the Transportation Research Board Annual Meeting, Washington, DC, January, 2003), CD-ROM.

28. Susan L. Cutter and Minhe Ji, "Trends in US Hazardous Materials Transportation Spills," *Professional Geographer* 49, no. 3 (1997): 318–331; Barkan, Dick, and Anderson, "Railroad Derailment Factors."

29. Jeremy F. Plant, "Terrorism and the Railroads: Redefining Security in the Wake of 9/11," *Journal of Policy Research* 21, no. 3 (2004): 293–297.

30. See Request for Comments, 69 Fed. Reg. at 50988–50994.

31. On this point, see the discussion of Ulrich Beck in chapter 3.

32. See Rick Hind, letter to Senators Collins and Lieberman, September 15, 2005; U.S. Federal Railroad Agency, "Regulatory Assessment, Regulatory Flexibility Analysis," in *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (April 2008), 29; Friends of the Earth, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (May 15, 2007).

33. Plant, "Terrorism and the Railroads," 299.

34. In addition to hazmat security, AAR's security task force examined the protection of physical infrastructure, operational security, interaction with the military, and communication and information technology security. Ibid., 298.

35. Chemical Security Act of 2001, S. 1602, 107th Cong. (2001).

36. Eric Pianin, "Toxic Chemicals' Security Worries Officials; Widespread Use of Industrial Materials Makes Them Potential Target of Terrorists," *Washington Post*, November 12, 2001.

37. Quoted in Ibid.

38. Ibid.

39. Quoted in Ibid.

40. Quoted in Ibid.

41. Ibid.

42. Aviation and Transportation Security Act, Pub. L. No. 107–171, 115 Stat. 597 (2001).

43. AAR, "Submitted Comments," comment on *Hazardous Materials*, No. RSPA-2004-18730 (February 16, 2005), 3–4.

44. Advisory Notice, Enhancing the Security of Hazardous Materials in Transportation, 31 Fed. Reg. 6963–6966 (February 14, 2002).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

45. Plant, "Terrorism and the Railroads," 299.

46. Federal Bureau of Investigation, "FBI Distributed through the NLETS Communications System," press release, October 23, 2002, https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-distributed-through-the-nlets-communications-system.

47. For an overview of the position of the environmental groups, see Greenpeace, "Submitted Comments," comment on *Hazardous Materials*, No. RSPA-2004-18730 (October 18, 2004); Friends of the Earth, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730. For the Sierra Club's position, see CSX Transp., Inc v. Williams, No. 05–338, 2005 U.S. Dist. LEXIS 6569 (D.D.C. Apr. 18, 2005).

48. "Hell on Wheels"; Greenpeace, "Re-routing Will Eliminate."

49. Homeland Security Act of 2002. Pub. Law. No. 107–296, § 1710–11, 116 Stat. 2135, 2319–20 (2002).

50. Final Rule: Hazardous Materials: Security Requirements for Offerors and Transporters of Hazardous Materials, 68 Fed. Reg. 14511 (March 25, 2003).

51. Ibid., 14510–14521.

52. Ibid.

53. Greenpeace, "Submitted Comments," comment on *Hazardous Materials*, No. RSPA-2004-18730.

54. Greenpeace charged that the Bush administration's close ties with industry interfered with more substantive regulations. At the time, former CSX chairman John W. Snow served as treasury secretary. Spencer S. Hsu, "D.C. May Ban Hazardous Shipments; Anti-terror Proposal Pits Environmentalists against Rail Officials," *Washington Post*, January 24, 2004. On the relationship between the rail and chemical industries and regulation, see Public Citizen, *Homeland Unsecured: The Bush Administration's Hostility to Regulation and Ties to Industry Leave America Vulnerable* (Washington, DC: Public Citizen, 2004), https://www.citizen.org/sites/default/files/acf1b7.pdf.

55. Paolino, "All Aboard," 158–159.

56. Regarding the exceptional status of Washington, DC, as a terrorist target, Councilwoman Kathy Patterson noted that travelers in and out of Reagan National Airport alone face unique restrictions. Only when arriving or departing from Reagan are travelers prevented from leaving their seats for 30 minutes before takeoff and landing. Patterson, "Statement on Introduction."

57. *CSX Transp*., 2005 U.S. Dist. LEXIS 6569, at *16 (D.D.C. Apr. 18, 2005).

58. Hsu, "D.C. May Ban Hazardous Shipments."

59. Terrorism Prevention and Safety in Hazardous Materials Transportation Act of 2003, B15–0525, D.C. City Council (2003); Terrorism Prevention and Safety in Hazardous Materials Transportation Emergency Act of 2004, B15–1100, D.C. City Council (2004); Spencer S. Hsu and Sari Horwitz, "Hazmat Rerouting Decision Delayed; White House Accused of 'Playing Politics' over DC Rail Line," *Washington Post*, October 25, 2004; Greenpeace, "Submitted Comments," comment on *Hazardous Materials*, No. RSPA-2004-18730.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

60. In August 2004, DOT issued a request seeking comments on how to improve the security of hazmat transportation. Though comments were due by October, DOT did not take any further steps to introduce new regulations. Request for Comments, 69 Fed. Reg. at 50988–50994; Hsu and Horwitz, "Hazmat Rerouting Decision Delayed."

61. Patterson, "Statement on Introduction."

62. Terrorism Prevention in Hazardous Materials Transportation Emergency Act of 2005, DC Code §§8-1421-8-1426 (2005); Paolino, "All Aboard," 154.

63. DC Code §8–1421.

64. Ibid.

65. Patterson, "Statement on Introduction."

66. DC Code §§8–1423, 8–1424.

67. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569 at *16 (D.D.C. Apr. 18, 2005).

68. Specifically, the DC Council wanted CSX to enter into an interchange agreement, which would have allowed Norfolk Southern Railway to carry identified hazardous cargoes on its line 50 miles west of the district. Patterson, "Statement on Introduction."

69. Elizabeth A. Moore, "Federalism vs. Terrorism: Damaging DC's Defense against Chemical Attacks in *CSX Transportation, Inc. v. Williams*," note, *George Washington Law Review* 74 (2005–2006): 772.

70. Others joining CSX include the American Petroleum Institute, Chlorine Chemistry Council, Chlorine Institute, Fertilizer Institute, National Association of Chemical Distributors, and the Sulphur Institute. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569.

71. Wabash, St. Louis & Pacific Railway Company v. Illinois, 118 U.S. 557 (1886).

72. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569, at *3.

73. Ibid., *4–5.

74. For review of the questions raised in *CSX v. Williams*, see Moore, "Federalism vs. Terrorism"; Paolino, "All Aboard"; Chris McChesney, "Toxic Trains: Chemical Transportation Regulation, Terrorism, and the U.S. Capitol," *Sustainable Development Law & Policy* 6, no. 3 (2006): 30–32, 81.

75. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569, at *16–17.

76. Moore, "Federalism vs. Terrorism," 772.

77. 49 U.S.C. § 20106 (2012).

78. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569, at *28–29.

79. 49 U.S.C. § 20106 (2012); see also ibid., *22.

80. 49 U.S.C. § 20106 (2012).

81. 49 U.S.C. § 5125(a) (2012); see also *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569, at 24.

82. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

83. Ibid., *31–32.

84. Ibid., *37.

85. The court notes that DOT estimates that compliance with HM-232 will occupy 50 hours of work—roughly one week of work by a single employee. In the court's reading, such a minor effort can hardly be deemed to "cover" the complex issue of hazardous materials security. Ibid.

86. Ibid.

87. Ibid.

88. Ibid.

89. Ibid., *39–41.

90. CSX Transp., Inc. v. Williams, 406 F.3d 667, 669 (D.C. Cir. 2005).

91. Ibid., 672.

92. Ibid.

93. Ibid., 673.

94. Ibid., 672.

95. Ibid.

96. Ibid., 673.

97. Ibid.

98. Ibid

99. The concurring opinion of Judge Karen LeCraft Henderson notes that the act would also be preempted by the Hazardous Materials Transportation Act on similar ground. Ibid. at 674 (Henderson, K.L., concurring).

100. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–152, 112 Stat. 266 (2007).

101. See *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569 (D.D.C. 2005) (No. 05–338).

102. See Notice of Proposed Rulemaking: Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments, 71 Fed. Reg. 76834–76850 (December 21, 2006); Interim Final Rule, 73 Fed. Reg. 20752–20773; Final Rule: Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments, 73 Fed. Reg. 72182–72194 (November 26, 2008).

103. *CSX Transp.*, 2005 U.S. Dist. LEXIS 6569, at *37.

104. Notice of Proposed Rulemaking, 71 Fed. Reg. at 76842.

105. Ibid., 76848.

106. Ibid., 76842.

107. Ibid., 76834.

108. Ibid., 76839–76840.

109. Ibid., 76842.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

110. Ibid., 76849.

111. Ibid.

112. Ibid., 76844.

113. See Greenpeace, "Re-routing Will Eliminate"; Friends of the Earth, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (February 18, 2007); City of Baltimore, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (February 20, 2007); State of Connecticut, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (March 9, 2007); District of Columbia, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (February 16, 2007); City of Cleveland, "Submitted Comments," comment on *Hazardous Materials*, No. PHMSA-RSPA-2004-18730 (February 16, 2007).

114. Notice of Proposed Rulemaking, 71 Fed. Reg. at 76834, 76848.

115. Interim Final Rule, 73 Fed. Reg. at 20752, 20761.

116. Final Rule, 73 Fed. Reg. at 72182, 72185.

117. Interim Final Rule, 73 Fed. Reg. at 20755–20756.

118. See note 113.

119. See Carol. D. Leonnig, "Congress Approves Rail Cargo Measure; Hazardous Matter Would Be Banned on Lines in DC," *Washington Post*, July 29, 2007; Friends of the Earth, "Congress Passes Toxic Rail Protections for Major Cities," news release, July 30, 2007, https://foe.org/2008-10-congress-passes-toxic-rail-protections-for-major-cit/.

120. Implementing Recommendations of the 9/11 Commission Act of 2007.

121. Ibid., § 1551(a).

122. Ibid., § 1551(d).

123. Ibid., § 1551(c)(h).

124. Previous attempts at passing rerouting legislation failed. See, for example, the Extremely Hazardous Materials Rail Transportation Act of 2005, S. 773, 109th Cong. (2005); Hazardous Materials Vulnerability Reduction Act of 2005, S. 1256, 109th Cong. (2005); 9/11 Commission Recommendations Implementation Act of 2006, S. 2412, 109th Congress.

125. Final Rule, 73 Fed. Reg. at 72182, 72186.

126. Interim Final Rule, 73 Fed. Reg. at 20752, 20771–20773.

127. Final Rule, 73 Fed. Reg. at 72183.

128. Interim Final Rule, 73 Fed. Reg. at 20761–20762, 20766–20768.

129. Ibid., 20766.

130. On the frustrations with the regulations, see Friends of the Earth, "Friends of the Earth Blasts Bush Admin Railroad Routing Regs," news release, April 16, 2008, https://foe.org/2008-11-friends-of-the-earth-blasts-bush-admin-railroad-rout/.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

131. Final Rule: Hazardous Materials: Enhanced Tank Car Standards and Operational Controls for High-Hazard Flammable Trains, 80 Fed. Reg. 26664–26750 (May 8, 2015).

132. Final Rule, 80 Fed. Reg. at 26665.

133. Transportation Safety Board of Canada, "Runaway and Main-Track Derailment: Montreal, Maine and Atlantic Railway Freight Train MMA-002 Mile 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013," *Railway Investigation Report*, No. R13D0054, August 20, 2014, 1–3.

134. National Transportation Safety Board, "CSXT Petroleum Crude Oil Derailment and Hazardous Materials Release," *Railroad Accident Brief*, March 2, 2016.

135. Final Rule, 80 Fed. Reg. at 26665.

136. Michael Laris and Peter Hermann, "Train Derails in Downtown Lynchburg, Leaving Crude Burning on James River," *Washington Post*, April 30, 2014; Cassidy Craighill, "One Year after Lac-Megantic, Residents Gather to Stop Oil Trains," Greenpeace, July 7, 2014, https://www.greenpeace.org/usa/one-year-lac-megantic-residents-gather-stop-oil-trains/.

137. Final Rule, 80 Fed. Reg. at 26643.

138. Final Rule, 80 Fed. Reg.

139. Pianin, "Toxic Chemicals' Security Worries Officials."

140. Ibid.

Chapter 6

1. U.S.-Canada Power System Outage Task Force (hereafter "Power System Outage Task Force"), *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, 65–66.

2. Randy Kennedy, "Thousands Stranded on Foot by Crippled Trains, Crawling Buses and Traffic Gridlock," *New York Times*, August 15, 2003; James Barron, "Power Surge Blacks Out Northeast," *New York Times*, August 15, 2003; Janny Scott, "In Subways, in Traffic, in Elevators: All Stuck," *New York Times*, August 15, 2003.

3. Power System Outage Task Force, *Final Report*, 1–11, 73–74, 103–107.

4. Ibid., 45–49.

5. "Major Power Outage Hits New York, Other Large Cities," CNN, August 15, 2003, http://www.cnn.com/2003/US/08/14/power.outage/.

6. Barron, "Power Surge."

7. "Energy Bill Leaves U.S. in Policy Limbo," *Toronto Star*, August 13, 2005.

8. See David Owens, Edison Electric Institute, *Statement for the Record*, submitted to the Subcommittee on Energy and Power, Committee on Commerce, U.S. House of Representatives, July 22, 1999, 69.

9. Power System Outage Task Force, *Final Report*, 10.

10. Owens, *Statement for the Record*, 69.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

11. T. J. Glauthier, Department of Energy, *Statement for the Record*, submitted to the Subcommittee on Energy and Power, Committee on Commerce, U.S. House of Representatives, October 5, 1999, 20.

12. The NERC consensus language appeared in a number of bills during the late 1990s and early 2000s. For example, see Sec. Title II—Electric Reliability, Electricity Competition and Reliability Act, H.R. 2944, 106th Cong. (1999).

13. See *The Electricity Competition and Reliability Act, Hearing Before Subcomm. on Energy and Power of H. Comm. Commerce*, 106th Cong. (1999).

14. *Toronto Star*, "Energy Bill Leaves U.S. in Policy Limbo."

15. GAO, *Energy Task Force: Process Used to Develop the National Energy Policy*, GAO-03-894 (Washington, DC, 2003).

16. Ibid., 4–5.

17. Barton Gellman, *Angler: The Cheney Vice Presidency* (New York: Penguin, 2008): 91–92.

18. "Court Upholds Secrecy for Cheney's Energy Task Force," *Chicago Tribune*, May 11, 2005.

19. Michael Abramowitz and Steven Mufson, "Paper Detail Industry's Role in Cheney's Energy Report," *Washington Post*, July 18, 2007; Gellman, *Angler*, 92.

20. Gellman, *Angler*, 81–108.

21. Abramowitz and Mufson, "Paper Detail Industry's Role"; National Energy Policy Development Group (NEPDG), *National Energy Policy* (Washington, DC: GPO, 2001).

22. NEPDG, *National Energy Policy*, 7-6.

23. Subcommittee on Energy and Power, Committee on Commerce, U.S. House of Representatives, October 5, 1999, 51 (statement of James Hoecker, Chairman, FERC).

24. In terms of megawatts and people affected, the 2003 blackout far outstripped pervious blackouts, including the 1965 Northeast blackout and the New York City blackout of 1977. The 1965 blackout, for example, affected an estimated 30 million people and involved 20,000 megawatts. For historical comparisons with other blackouts, see Power System Outage Task Force, *Final Report*, 1–2, 73–74, 103–107.

25. Ibid., 1.

26. Ibid., 1–2.

27. Phase I investigated the causes of the blackout; phase II examined the requirements needed to prevent future blackouts. Ibid., 1

28. Ibid., 1.

29. For a complete listing of working-group members, see ibid., app. A, 175–177.

30. Power System Outage Task Force, *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, November 2003; Power System Outage Task Force, *Final Report*.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

31. Power System Outage Task Force, *Final Report*, 18–19, 45–102.

32. Ibid., 18–19, 45.

33. Ibid., 18–19, 48.

34. Ibid., 17–20, 22.

35. The reprioritization of infrastructure networks as targets and the circulation of worst-case scenarios led accidents, such as the collapse of portions of the I-35 bridge in Minneapolis in 2007, to be interpreted as possible terrorist actions. See Jon Elsen and Libby Sander, "Dozens Missing as Minneapolis Search Efforts Are Halted," *New York Times*, August 2, 2007.

36. Rashbaum, "Responding to a Blackout."

37. Power System Outage Task Force, *Interim Report*, 96.

38. Elisabeth Bumiller, "Bush Doesn't Let Blackout Upset Lunch with Troops," *New York Times*, August 15, 2003.

39. Power System Outage Task Force, *Final Report*, 134–135.

40. Ibid.

41. Ibid., 1.

42. Ibid.

43. Ibid., 134–135.

44. Ibid., 131–138.

45. Ibid., 132.

46. Ibid.

47. Ibid.

48. The report notes that FirstEnergy, a key player during the 2003 blackout, had significant problems with the Slammer worm in January 2003. The worm attacked control systems at FirstEnergy's idle Davis-Besse nuclear plant. Ibid., 132–133.

49. There is confusion and overlapping usage within the report itself. See, for example, ibid., 23.

50. Ibid.

51. NEPDG, *National Energy Policy*, 8-1-8-21.

52. Ibid. 7-16.

53. Power System Outage Task Force, *Final Report*, 8–9, 13.

54. Ibid.

55. Ibid.

56. Michael Assante, North American Electric Reliability Corporation (NERC), "RE: Critical Cyber Asset Identification," letter to industry stakeholders, April 7, 2009, http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf.

57. FERC, "Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Reliability Corporation's Proposed Mandatory

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Reliability Standards on Critical Infrastructure Protection," in *Mandatory Reliability Standards for Critical Infrastructure Protection*, No. RM06-22-000 (Washington, DC: FERC, December 11, 2006), 7 (hereafter cited as "Staff Preliminary Assessment").

58. Assante, "RE: Critical Cyber Asset Identification."

59. Ibid.

60. Power System Outage Task Force, *Final Report*, 141–142.

61. Ibid., 10.

62. Power System Outage Task Force, *Final Report*, 10, 20–22.

63. Ibid., 139–143.

64. Ibid., 141–142.

65. Ibid., 140–142.

66. Ibid.

67. Ibid., 164. See NERC, "Urgent Action Standard 1200—Cyber Security," August 13, 2003, in *Mandatory Reliability Standards for the Bulk-Power System*, No. RM06-16-000 (Washington, DC: FERC, April 4, 2006).

68. FERC, "Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Council's Proposed Mandatory Reliability Standards," in *Mandatory Reliability Standards*, No. RM06-16-000 (May 11, 2006), 34–41 (hereafter cited as "Staff Preliminary Assessment").

69. Power System Outage Task Force, *Final Report*, 163–164.

70. Energy Policy Act of 2005, Pub. L. No. 109–58, 119 Stat. 594 (2005).

71. Jim VendeHei and Justi Blum, "Bush Signs Energy Bill, Cheers Steps toward Self-Sufficiency," *Washington Post*, August 9, 2005.

72. Ibid.

73. Gellman, *Angler*, 107.

74. Michael Abramowitz and Steven Mufson, "Paper Detail Industry's Role in Cheney's Energy Report," *Washington Post*, July 18, 2007.

75. Quoted in VendeHei and Blum, "Bush Signs Energy Bill."

76. George W. Bush, "President Signs Energy Policy Act," August 8, 2005, transcript, The White House, https://georgewbush-whitehouse.archives.gov/news/releases/2005/08/20050808-6.html.

77. Pub. L. No. 109–58 § 1211 (2005).

78. Ibid.

79. Ibid.

80. Ibid.

81. Ibid.

82. Ibid.

83. Ibid.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

84. Ibid.

85. Ibid.

86. NERC, "Request of the North American Electric Reliability Council and North American Electric Reliability Corporation for Approval of Reliability Standards," in *Mandatory Reliability Standards*, No. RM06-16-000 (April 4, 2006); NERC, "Request of the North American Electric Reliability Council and North American Electric Reliability Corporation for Certification as the Electric Reliability Organization," in *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, No. RM05-30-000 (Washington, DC: FERC, April 4, 2005).

87. FERC, Order No. 672, *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* F.E.R.C. ¶ 31,204 (2006) (to be codified at 18 C.F.R. pt. 39).

88. Ibid., 48, 54–60.

89. Ibid., 105–140.

90. Ibid., 10.

91. For a discussion of industry claims in favor of a strong ERO unencumbered by substantive review and FERC's rejection of this position, see ibid., 50–54, 136–138.

92. Ibid., 136–138.

93. See, for example, the comment of PacifiCorp in ibid., 136.

94. Ibid., 107–109.

95. Ibid.

96. Ibid.

97. Ibid., 148–150.

98. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,*

No. RM06-22-000, 1.

99. Ibid., 4–5; NERC, "Standard Development Roadmap," in *Mandatory Reliability Standards*, No. RM06-22-000 (n.d.); NERC, "Cyber Security," in *Mandatory Reliability Standards*, No. RM06-22-000 (n.d).

100. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 8–14.

101. FERC's objections and analysis are outlined in ibid.; FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-16-000, 34–41; Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection, 72 Fed. Reg. 43970 (August 6, 2007).

102. The approval process for reliability standard involves four general steps: (1) the ERO develops consensus standards through working groups and balloting; (2) FERC conducts a preliminary technical review of the proposed standard (or standards) and issues a report detailing findings; (3) FERC issues a formal

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Notice of Proposed Rulemaking and opens the standard to public review and discussion; (4) FERC issues an order to either accept or remand the standard.

103. NERC, "Cyber Security: Standard CIP-002–1–CIP-009–1," in *Mandatory Reliability Standards*, No. RM06-22-000 (August 28, 2006).

104. NERC, "Definitions of Terms Used in Standard," in *Mandatory Reliability Standards*, No. RM06-22-000 (n.d.).

105. Ibid.

106. Ibid.

107. The initial standards did not cover local distribution. Each CIP standard identified 11 responsible entities subject to the rules: reliability coordinator, balancing authority, interchange authority, transmission service provider, transmission owner, transmission operator, generator operator, load-serving entity, NERC, and regional reliability organizations. NERC, "Cyber Security: Standard CIP-002–1–CIP-009–1."

108. NERC, "Definitions of Terms"; NERC, "Cyber Security: Standard CIP-002–1—CIP-009–1."

109. Notice of Proposed Rulemaking, 72 Fed. Reg. 43970, 43971–43972.

110. NERC, "Cyber Security: Standard CIP-002–1—CIP-009–1."

111. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards*, No. RM06-16-000, 34–41; NERC, "Urgent Action Standard 1200."

112. NERC, "Cyber Security: Standard CIP-002–1—CIP-009–1."

113. NERC, "Frequently Asked Questions (FAQs): Cyber Security Standards CIP–002–1 through CIP–009–1," in *Mandatory Reliability Standards*, No. RM06-22-000 (March 2006).

114. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 8–10; Notice of Proposed Rulemaking, 72 Fed. Reg. 43970, 43977.

115. NERC, "FAQs."

116. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 8–10; Notice of Proposed Rulemaking, 72 Fed. Reg. at 43977–43978.

117. See comments at Notice of Purposed Rulemaking, 72 Fed. Reg at 43977; Final Rule: Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368 (Feb, 7, 2008) (to be codified at 18 C.F.R. pt. 40); Pacific Gas and Electric, "Submitted Comments," comment on *Mandatory Reliability Standards*, No. RM06-22-000 (February 12, 2007), 5–6.

118. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43976; Final Rule, 73 Fed. Reg. at 7381; Progress Energy, Inc., "Submitted Comments," comment on *Mandatory Reliability Standards*, No. RM06-22-000 (February 12, 2007), 3.

119. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 8–10; Notice of Proposed Rulemaking, 72 Fed. Reg. at 43976–43978; Final Rule, 73 Fed. Reg. at 7381–7383.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

120. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 10.

121. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43977. On the general challenges of interdependent security, see Geoffrey Heal et al., "Interdependent Security in Interconnected Networks," in Auerswald et al., *Seeds of Disaster*, 258–276.

122. Final Rule, 73 Fed. Reg. at 7380.

123. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43977.

124. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 3, 20–21, 32.

125. NERC, "Cyber Security: Standard CIP-002–1—CIP-009–1."

126. Ibid.

127. Ibid.

128. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43979.

129. Final Rule, 73 Fed. Reg. 7368, 7383.

130. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43980; FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 3, 20.

131. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43980.

132. Ibid.

133. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 20–21.

134. Ibid.

135. Ibid., 11; Notice of Proposed Rulemaking, 72 Fed. Reg. at 43974; Final Rule, 73 Fed. Reg. 7368, 7375.

136. Final Rule, 73 Fed. Reg. at 7374.

137. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43974.

138. Ibid., 43981.

139. Ibid., 43974.

140. NERC, "Cyber Security: Standard CIP-002–1—CIP-009–1."

141. Notice of Proposed Rulemaking, 72 Fed. Reg. at 43974.

142. FERC, "Staff Preliminary Assessment," in *Mandatory Reliability Standards,* No. RM06-22-000, 11; Notice of Proposed Rulemaking, 72 Fed. Reg. at 43974; Final Rule, 73 Fed. Reg. at 7375.

143. NERC, "Request of the North American Electric Reliability Corporation for Approval of Violation Risk Factors for Version 1 Reliability Standards," No. RR07, March 23, 2007, https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Version_1_VRF_filing_3-23-07_FINAL.pdf, 8–9.

144. NERC, "Sanction Guidelines of the North American Electric Reliability Corporation," January 15, 2008, app. 4B, accessed July 30, 2019, https://www

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

.nerc.com/pa/comp/Resources/ResourcesDL/Appendix4B_Sanctions_Guidelines_Effective_20080115.pdf.

145. For a description of the different categories of violation risk factors, see NERC, "Violation Risk Factors," 8–9.

146. NERC, "Sanction Guidelines," 19.

147. Final Rule, 73 Fed. Reg. at 7440.

148. Ibid.

149. Ibid., 7441–7442; Notice of Proposed Rulemaking, Final Rule, 72 Fed. Reg., 43970, 44010–44013.

150. Notice of Proposed Rulemaking, 72 Fed. Reg. at 44005–44006; Final Rule, 73 Fed. Reg. at 7440–7442.

151. Note: each CIP reliability standard contained multiple requirements and subrequirements, each receiving a violation risk factor. For a list of proposed violation risk factors and FERC's recommend changes, see NERC, "Violation Risk Factors"; Notice of Proposed Rulemaking, 72 Fed. Reg. at 44010–44013.

152. See Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011).

153. For example, FERC directed NERC to provide further guidance as to what a risk-based methodology might entail and called for the reworking of CIP-005 to specifically include a direction to regulated parties to adopt defense-in-depth posture (layering of multiple security procedures). Final Rule, 73 Fed. Reg. at 7376–7384, 7394, 7417, 7440–7442. See also Ryan Ellis, "Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?" *IEEE Security & Privacy* 12, no. 6 (2014): 48–54.

154. See Revised Critical Infrastructure Protection Reliability Standards, 154 FERC ¶ 61,037 (2016); Ellis, "Regulating Cybersecurity."

Conclusion

1. On spatial dependency and risk, see Perrow, *Next Catastrophe*, 297–298.

2. Monahan, "Questioning Surveillance and Security," 1–26.

3. Quoted in Anne Gearan, "For President Trump, 'National Security' Can Mean Just about Anything," *Washington Post*, August 22, 2018.

Coda

1. Quoted in Hendrik Hertzberg, "Unwinding 'Unwitting,'" *New Yorker*, June 20, 2013, https://www.newyorker.com/news/daily-comment/unwinding-unwitting.

2. For an insider account of the early days of the Snowden revelations, see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Holt, 2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (New York: Vintage, 2014).

3. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian* (UK), June 6, 2013.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

4. Glenn Kessler, "James Clapper's Least Untruthful Statement to the Senate," *Washington Post*, June 11, 2013, http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.

5. Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013; Greenwald, *No Place to Hide*.

6. Perlroth, Larson, and Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web."

7. For a discussion and overview of the market for flaws, see Trey Herr and Ryan Ellis, "Disrupting Malware Markets," in *Cyber Insecurity: Navigating the Perils of the Next Information Age*, ed. Richard Harrison and Trey Herr (New York: Rowman & Littlefield, 2016), 105–122.

8. Brian Fung, "The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities," *Washington Post*, August 31, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

9. Susan Landau provided a prescient warning with respect to the creation of surveillance technologies and capabilities before the Snowden disclosures. Designing technologies or systems with built-in wiretapping capabilities enhance a state's ability to collect information, but it undermines security and creates new paths for misappropriation and malicious use. Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2013).

10. For a window into the policy debates and contradictions found in these competing efforts, see David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018).

11. Bruce Schneier, "The NSA Is Hoarding Vulnerabilities," *Schneier on Security*, August 2016, https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

12. Ibid.

13. For a detailed examination of the tensions between offense and defense (and a discussion of the limitations of these terms) see Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford University Press, 2016).

14. On the risks of escalation in cyberspace, see Herb Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (2012): 46–70.

15. This was a fear within the Obama administration that largely came to pass. After launching Stuxnet—a campaign to degrade and disrupt Iranian nuclear capabilities—other countries, including Iran, ramped up malicious activity in cyberspace. See Sanger, *Perfect Weapon*; Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: Signal, 2013).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

16. For a rich examination of the possibilities of reuse and appropriation, see Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press), 160–192.

17. David E. Sanger, "'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?," *New York Times*, August 16, 2016, https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html.

18. Nicholas Weaver, "NSA and the No Good, Very Bad Monday," *Lawfare*, August 16, 2016, https://www.lawfareblog.com/very-bad-monday-nsa-0.

19. Andy Greenberg, "The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days," *Wired*, August 17, 2016, https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/; Weaver, "NSA and the No Good, Very Bad Monday."

20. Scott Shane, Nicole Perlroth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core," *New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

21. Lily Hay Newman, "The Leaked NSA Spy Tool That Hacked the World," *Wired*, March 7, 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

22. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

23. Iain Thomson, "74 Countries Hit by NSA-Powered WannaCrypt Ransomware Backdoor: Emergency Fixes Emitted by Microsoft for WinXP+," *Register*, May 13, 2017, https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/.

24. Greenberg, "The Untold Story of NotPetya."

25. Ibid.

26. Ibid.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Bibliography

Agamben, Giorgio. *State of Exception*. Translated by Kevin Attell. Chicago: University of Chicago Press, 2003.

Albert, Reka, Hawoong Jeong, and Albert-László Barabási. "Error and Attack Tolerance of Complex Networks." *Nature* 406 (2000): 378–382.

Aldrich, Mark. *Death Rode the Rails: American Railroad Accidents and Safety, 1828–1965*. Baltimore: Johns Hopkins University Press, 2006.

Aldrich, Mark. "Regulating Transportation of Hazardous Substances: Railroads and Reform, 1883–1930." *Business History Review* 26, no. 2 (2002): 267–297.

Anderson, Douglas D. *Regulatory Politics and Electric Utilities: A Case Study in Political Economy*. Boston: Augurn, 1981.

Aradau, Claudia. "Security That Matters: Critical Infrastructure and Objects of Protection." *Security Dialogue* 41, no. 5 (2010): 491–514.

Arthur D. Little. "A Description of the Postal Service Today: Appendix A to the General Contract." Annex contractor's report. Vol. 4, *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization. Washington, DC: Government Printing Office, 1968, 6–69.

Arthur D. Little. "The U.S. Post Office and Organizational Options for its Improvement." Annex contractor's report. Vol. 1, *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization. Washington, DC: Government Printing Office, 1968.

Aspen Institute Justice and Society Program and the Annenberg Public Policy Center of the University of Pennsylvania. *Alarms Unheeded: Lessons on the 13th Anniversary of the Final Hart-Rudman Report*. 2014. https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/Alarms-Unheeded.pdf.

Aspray, William. "Edwin L. Harder and the Anacom: Analog Computing at Westinghouse." *IEEE Annals of the History of Computing* 15, no. 2 (1993): 35–52.

Assante, Michael J., and Robert M. Lee. "The Industrial Control System Kill Chain." SANS Institute. October 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Association of American Railroads. *Hazmat Transportation by Rail: An Unfair Liability*. Washington, DC, September 2009, http://thehill.com/sites/default/files/aar_hazmatbyrailseptember2009_0.pdf.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Association of American Railroads. *The Impact of the Staggers Rail Act of 1980*. Washington, DC, 2010. Accessed November 3, 2010. https://web.archive.org/web/20101103064437/http://aar.org/~/media/aar/backgroundpapers/impactofthestaggersrailactof1980.ashx/.

Auerswald, Philip, Lewis Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan, eds. *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerabilities*. Cambridge: Cambridge University Press, 2006.

Averch, Harvey, and Leland L. Johnson. "Behavior of the Firm under Regulatory Constraint." *American Economic Review* 52, no. 5 (1962): 1052–1069.

Bailey, Elizabeth E. "Price and Productivity Change Following Deregulation: The US Experience." *Economic Journal* 96, no. 381 (1986): 1–17.

Barabási, Albert-László. *Linked: The New Science of Networks*. New York: Perseus, 2002.

Barkan, Christopher P. L., C. Tyler Dick, and Robert Anderson. "Analysis of Railroad Derailment Factors Affecting Hazardous Materials Transportation Risk." Presented at the Transportation Research Board Annual Meeting, Washington, DC, January 2003. CD-ROM.

Barnes, Ken, Briam Johnson, and Reva Nickelson. *Review of Supervisory Control and Data Acquisition Systems (SCADA)*. Idaho Falls: Idaho National Engineering and Environmental Laboratory, 2004. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.5922&rep=rep1&type=pdf.

Bauman, Zygmunt, and David Lyon. *Liquid Surveillance: A Conversation*. Malden, MA: Polity, 2013.

Baxter, Vern K. *Labor and Politics in the U.S. Postal Service*. New York: Plenum Press, 1994.

Beck, Ulrich. "Global Risk Politics." *Political Quarterly* 68 (1997): 18–33.

Beck, Ulrich. "The Reinvention of Politics." In Beck, Giddens, and Lash, *Reflexive Modernization*, 1–55.

Beck, Ulrich. *Risk Society: Towards a New Modernity*. Translated by Mark Ritter. Thousand Oaks, CA: Sage, 1992.

Beck, Ulrich. "Self-Dissolution and Self-Endangerment of Industrial Society: What Does This Mean?" In Beck, Giddens, and Lash. *Reflexive Modernization*, 174–183.

Beck, Ulrich. *World at Risk*. Translated by Ciaran Cronin. Malden, MA: Polity, 2009.

Beck, Ulrich, Wolfgang Bonns, and Christoph Lau. "The Theory of Reflexive Modernization." *Theory, Culture & Society* 20, no. 2 (2016): 1–33.

Beck, Ulrich, Anthony Giddens, and Scott Lash. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Stanford, CA: Stanford University Press, 1994.

Beder, Sharon. *Power Play: The Fight to Control the World's Electricity*. New York: New Press, 2003.

Beniger, James. *The Control Revolution: Technological and Economic Origins of Information Society.* Cambridge, MA: Harvard UP, 1986.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press, 2006.

Bennett, Stuart. *A History of Control Engineering, 1800–1930*. New York: Institution of Electrical Engineers, 1979.

Bennett, Stuart. *A History of Control Engineering, 1930–1955*. London: Institution of Electrical Engineers, 1993.

Benson, Lee. *Merchants, Farmers, and Railroads: Railroad Regulation and New York Politics*. Cambridge, MA: Harvard University Press, 1955.

Benton-Short, Lisa. *The National Mall: No Ordinary Public Space*. Toronto: University of Toronto Press, 2016.

Bereskin, Gregory. "Regulation, Deregulation, and Reregulation in the Surface Transportation Industry." *Transportation in the New Millennium: State of the Art and Future Directions, Perspectives from Transportation Research Board Standing Committees*. Washington, DC: Transportation Research Board, 2000. http://onlinepubs.trb.org/onlinepubs/millennium/00097.pdf.

Biggart, Nicole W. "The Post Office as a Business: Ten Years of Postal Reorganization." *Policy Studies Journal* 11, no. 3 (1983): 483–491.

Bijker, Wiebe, Anique Hommels, and Jessica Mesman. "Studying Vulnerability in Technological Cultures." In Hommels, Mesman, and Bijker, *Vulnerability in Technological Cultures*, 1–26.

Birkland, Thomas A. *After-Disaster: Agenda Setting, Public Policy, and Focusing Events*. Washington, DC: Georgetown University Press, 1997.

Birkland, Thomas A. *Lessons of Disaster: Policy Change after Catastrophic Events*. Washington, DC: Georgetown University Press, 2006.

Bitzan, John D., and Theodore E. Keeler. "Economies of Density and Regulatory Change in the U.S. Railroad Freight Industry." *Journal of Law and Economics* 50, no. 1 (2007): 157–180.

Boardman, F. D. "Future Developments in the Control of Power Systems." *Philosophical Transactions of the Royal Society of London. Series A. Mathematical and Physical Sciences* 275, no. 1248 (1973): 243–253.

Borja, Elizabeth C. *Brief Documentary History of the Department of Homeland Security: 2001–2008*. Washington, DC: Department of Homeland Security, 2008. https://www.hsdl.org/?view&did=37027.

Boucher, J. N. "Real-Time Energy Control." Presented at the 1979 Power Industry Computer Applications Conference, Cleveland, OH. *IEEE Conference Proceedings*, 177–184.

Bowker, Geoffrey C., Karen Baker, Florence Millerand, and David Ribes. "Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment." In *International Handbook of Internet Research*, edited by J. Hunsinger, L. Klastrup, and M. Allen, 97–117. Dordrecht: Springer, 2009.

Branscomb, Lewis M., Mark Fagan, Philip Auerswald, Ryan N. Ellis, and Raphael Barcham. "Rail Transportation of Toxic Inhalation Hazards: Policy Responses to the Safety and Security Externality." Mossavar-Rahmani Center for Business &

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Government Regulatory Policy Program Working Paper, RPP-2010-01, Harvard University, 2010. http://www.hks.harvard.edu/m-rcbg/rpp/Working%20papers/Rail%20Transportation%20of%20TIH.pdf.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin, 2011.

Brown, D. F., W. E. Dunn, and A. J. Policastro. *A National Risk Assessment for Selected Hazardous Materials in Transportation*. Argonne, IL: Argonne National Laboratory, 2000.

Brown, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Fairfax, VA: Spectrum, 2006.

Brunton, Finn. *Spam: A Shadow History of the Internet*. Cambridge, MA: MIT Press, 2013.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford University Press, 2016.

Buzan, Barry, Ole Weaver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner, 1998.

Byres, Eric, Andrew Ginter, and Joel Langill. "How Stuxnet Spreads." Version 1. Tofino Security White Paper, February 22, 2011.

Capehart, Barney, ed. *Encyclopedia of Energy Engineering and Technology*. Boca Raton: CRC Press, 2007.

Carey, James. "A Cultural Approach to Communication." In *Communication as Culture: Essays on Media and Society*. New York: Routledge, 1992, 13–36.

Carlton, Dennis W., and Randal C. Picker. "Antitrust and Regulation." In *Economic Regulation and Its Reform: What Have We Learned?*, edited by Nancy L. Rose, 25–61. Chicago: University of Chicago Press, 2014.

Carpenter, Daniel P. *The Forging of Bureaucratic Autonomy: Reputations, Networks, and Policy Innovation in Executive Agencies, 1862–1928*. Princeton, NJ: Princeton University Press, 2001.

Center for Counterproliferation Research. "Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks." Working paper, Center for Counterproliferation Research, National Defense University, Washington, DC, 2002. http://www.fas.org/irp/threat/cbw/anthrax.pdf.

Centers for Disease Control and Prevention. "Bioterrorism Alleging Use of Anthrax and Interim Guidelines for Management—United States, 1998." *MMWR Weekly* 48, no. 4 (1999): 69–74.

Chandler, Alfred D., Jr. *The Visible Hand: The Managerial Revolution in American Business*. 1977. Reprint, Cambridge, MA: Harvard University Press, 1993.

Cieslak, Theodore J., and Edward M. Eitzen. "Clinical and Epidemiological Principles of Anthrax." *Emerging Infectious Diseases* 5, no. 4 (1999): 552–555.

Clark, Frederick C. *State Railroad Commissions, and How They May Be Made Effective*. Baltimore: Guggenheimer and Weil, 1891.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Cohen, Julie A. *The Grid: Biography of an American Technology*. Cambridge, MA: MIT Press, 2017.

Cohen, Robert H., Matthew Robinson, Renee Sheehy, Tom Sharkey, John Waller, and Spyros Xenakis. "The Conflict about Preserving Small Rural Post Offices: Differences in the Distribution of Pharmacies and Post Offices." Presented at Winton M. Blount Symposium on Postal History, Washington, DC, November 2006.

Cohn, Nathan. "Recollections of the Evolution of Realtime Control Applications to Power Systems." *Automation* 20, no. 2 (1984): 145–162.

Cohn, Nathan, S. B. Biddle, R. G. Lex, E. H. Preston, C. W. Ross, and D. R. Whitten. "On-Line Computer Applications in the Electric Power Industry." *Proceedings of the IEEE* 58, no. 1 (1970): 78–87.

Cole, Leonard A. *The Anthrax Letters: A Medical Detective Story*. Washington, DC: John Henry Press, 2003.

Collier, Stephen J., and Andrew Lakoff. "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem." In *The Politics of Securing the Homeland: Critical Infrastructure, Risk and (In)Security*, edited by Myriam Dunn and Kristian Søby Kristensen, 17–39. London: Routledge, 2008.

Collier, Stephen J., James Christopher Mizes, and Antina Von Schnitzler. "Preface: Public Infrastructures/Infrastructural Publics." *Limn*, no. 7 (July 2006).

Comarow, Murray B. "The Strange Story of Postal Reform." Washington, DC: Federal Trade Commission, 2007. Accessed June 5, 2013. https://web.archive.org/web/20130605181043/http://www.ftc.gov/os/comments/USPS%20Study/529332-00004.pdf.

Committee on Standards and Policies for Decontaminating Public Facilities Affected by Exposure to Harmful Biological Agents: How Clean Is Safe? *Reopening Public Facilities after a Biological Attack: A Decision Making Framework*. Washington, DC: National Academies Press, 2005.

Congressional Research Service. *The Postal Revenue Forgone Appropriation: Overview and Current Issues*, RS21025. Washington, DC: December 28, 2005.

Conkey, Kathleen. *The Postal Precipice: Can the U.S. Postal Service Be Saved?* Washington, DC: Center for the Study of Responsive Law, 1983.

Cortada, James W. *The Digital Hand*. Vol. 3, *How Computers Changed the Work of American Public Sector Industries*. New York: Oxford University Press, 2008.

Cuéllar, Mariano-Florentino. *Governing Security: The Hidden Origins of American Security Agencies*. Stanford, CA: Stanford University Press, 2013.

Cullinan, Gerald. *The United States Postal Service*. New York: Praeger, 1973.

Cutter, Susan L., and Minhe Ji. "Trends in US Hazardous Materials Transportation Spills." *Professional Geographer* 49, no. 3 (1997): 318–331.

Czamanski, Daniel. *Privatization and Restructuring of Electricity Provision*. Westport, CT: Praeger, 1999.

Day, Tom. "Mail Sanitization." Presentation to Mailers' Technical Advisory Committee. Washington, DC, November 8, 2001. https://ribbs.usps.gov/mtac/documents/tech_guides/.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Day, Tom. "Mail Sanitization Update." Presentation to Mailers' Technical Advisory Committee. Washington, DC, February 2002. https://ribbs.usps.gov/mtac/documents/tech_guides/.

DeGraaf, Leonard. "Corporate Liberalism and Electric Power System Planning in the 1920s." *Business History Review* 64, no. 1 (1990): 1–31.

Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal, 2013.

Derthick, Martha, and Paul Quirk. *The Politics of Deregulation*. Washington, DC: Brookings Institute, 1985.

Dewan, Puneet K., Alicia M. Fry, Kayla F. Laserson, Bruce C. Tierney, Conrad P. Quinn, James A. Hayslett, Laura N. Broyles et al. "Inhalational Anthrax Outbreak among Postal Workers, Washington, DC, 2001." *Emerging Infectious Diseases* 8, no. 10 (2002): 1066–1072.

Dewey, John. *The Public and Its Problems: An Essay in Political Inquiry*. New York: Henry Holt, 1927.

Donohue, Laura K. *The Cost of Counterterrorism: Power, Politics, and Liberty*. New York: Cambridge University Press, 2008.

Dougan, William R. "Railway Abandonments, Cross-Subsidies, and the Theory of Regulation." *Public Choice* 44, no. 2 (1984): 297–305.

Dragos Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." Version 2.20170613. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Dull, Peter M., Kathy E. Wilson, Bill Kournikakis, Ellen A. S. Whitney, Camille A. Boulet, Jim Y. W. Ho, Jim Ogston et al. "*Bacillus anthracis* Aerosolization Associated with a Contaminated Mail Sorting Machine." *Emerging Infectious Diseases* 8, no. 10 (2002): 1044–1047.

Early, E. D., W. E. Philips, and W. T. Shreve. "An Incremental Cost of Power-Delivered Computer." *Transactions of the American Institute of Electrical Engineers* 74, no. 3 (1955): 529–535.

Edwards, Paul. "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems." In *Modernity and Technology*, edited by Thomas J. Misa, Philip Brey, and Andrew Feenberg, 185–226. Cambridge, MA: MIT Press, 2003.

Ellis, Ryan. "Appropriating Risk: National Security and the Sunrise Powerlink Controversy." Paper presented at the National Communication Association Annual Convention, San Francisco, November 2011.

Ellis, Ryan. "Creating a Secure Network: The 2001 Anthrax Attacks and the Transformation of Postal Security." Supplement. *Sociological Review* 62 (2014): 161–182.

Ellis, Ryan. "Disinfecting the Mail: Disease, Panic, and the Post Office Department in Nineteenth-Century America." *Information & Culture: A Journal of History* 52, no. 4 (2017): 436–461.

Ellis, Ryan. "The Premature Death of Electronic Mail: The United States Postal Service's E-COM Program, 1978–1985." *International Journal of Communication* 7 (2013): 1949–1967.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Ellis, Ryan. "Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?" *IEEE Security & Privacy* 12, no. 6 (2014): 48–54.

Emery, E. David. "Regulated Utilities and Equipment Manufacturers' Conspiracies in the Electric Power Industry." *Bell Journal of Economics and Management Science* 4, no. 1 (1973): 322–337.

Emmons, William, III. "Franklin D. Roosevelt, Electric Utilities, and the Power of Competition." *Journal of Economic History* 53, no. 4 (1993): 880–907.

Energetics Inc. *Roadmap to Secure Control Systems in the Energy Sector*. Columbia, MD, 2006. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf.

Etheridge, Elizabeth. *Sentinel for Health: A History of the Centers for Disease Control*. Berkeley: University of California Press, 1992.

Ewald, Francois. "Insurance and Risk." In *The Foucault Effect: Studies of Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 197–210. Chicago: University of Chicago Press, 1991.

Federal Energy Regulatory Commission. *The Con Edison Power Failure of July 13 and 14, 1977*. Final Staff Report. Washington, DC, 1978.

Federal Energy Regulatory Commission. "Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Reliability Corporation's Proposed Mandatory Reliability Standards." In *Mandatory Reliability Standards for the Bulk-Power System*. No. RM06-16-000. Washington, DC: FERC, May 11, 2006.

Federal Energy Regulatory Commission. "Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection." In *Mandatory Reliability Standards for Critical Infrastructure Protection*. No. RM06-22-000. Washington, DC: FERC, December 11, 2006.

Fee, Elizabeth, and Theodore M. Brown. "Preemptive Biopreparedness: Can We Learn Anything from History?" *American Journal of Public Health* 91, no. 5 (2001): 721–726.

Fellmeth, Robert C. *The Interstate Commerce Omission: The Public Interest and the ICC*. New York: Grossman, 1970.

Flynn, Stephen. *The Edge of Disaster: Rebuilding a Resilient Nation*. New York: Random House, 2007.

Fortun, Kim. *Advocacy after Bhopal: Environmentalism, Disaster, New Global Orders*. Chicago: University of Chicago Press, 2001.

Foster Associates. "Rates and Rate-Making." Annex contractor's report. Vol. 2, *Towards Postal Excellence: Report of the General Contractor*, President's Commission on Postal Organization. Washington, DC: Government Printing Office, 1968.

Fowler, Dorothy G. *Unmailable: Congress and the Post Office*. Athens: University of Georgia Press, 1977.

Friedlaender, Ann F. *The Dilemma of Freight Rail Transportation*. Washington, DC: Brookings Institute, 1969.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Friedlaender, Ann F., and Richard H. Spady. *Freight Transport Regulation: Equity, Efficiency, and Competition in the Rail and Trucking Industries*. Cambridge, MA: MIT Press, 1981.

Friedlander, Gordon. "Computer-Controlled Power Systems: Part II—Area Controls and Load Dispatch." *IEEE Spectrum* 2, no. 5 (May 1965): 72–91.

Fuller, Wayne E. *The American Mail: Enlarger of the Common Life*. Chicago: Chicago University Press, 1972.

Fuller, Wayne E. *RFD: The Changing Face of Rural America*. Bloomington: Indiana University Press, 1964.

Gaskins, Darius W. "Regulation of Freight Railroads in the Modern Era: 1970–2010." *Review of Network Economics* 7, no. 4 (2008). doi:10.2202/1446–9022.1162.

Geertz, Clifford. "Thick Description: Toward an Interpretive Theory of Culture." In *The Interpretation of Cultures: Selected Essays*, 3–30. New York: Basic, 1973.

Gellman, Barton. *Angler: The Cheney Vice Presidency*. New York: Penguin, 2008.

Gibert, Pam. "Using Intelligent Technology for Mail Security." Presentation to Mailers' Technical Advisory Committee. Washington, DC, November 8, 2001. https://ribbs.usps.gov/mtac/documents/tech_guides/.

Giddens, Anthony. "Living in a Post-traditional Society." Beck, Giddens, and Lash, *Reflexive Modernization*, 56–109.

Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press, 2018.

Ginsberg, Wendy. *US Postal Service Workforce Size and Employment Categories, 1987–2007*. Prepared by the Congressional Research Service, RS22864. Washington, DC: Library of Congress, 2008.

Goldsmith, Jack. *Power and Constraint: The Accountable Presidency after 9/11*. New York: Norton, 2012.

Gorman, Sean. *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Northampton, MA: Edward Elgar, 2005.

Gottron, Frank. *The U.S. Postal Service Response to the Threat of Bioterrorism through the Mail*. Prepared by the Congressional Research Service, RL31280. Washington, DC: Library of Congress, 2009.

Graham, Benjamin, and David Dodd. *Security Analysis: The Classic 1940 Edition*. 2nd ed. New York: McGraw-Hill, 2002.

Graham, Stephen. *Cities under Siege: The New Military Urbanism*. Brooklyn: Verso, 2011.

Graham, Stephen, ed. *Cities, War, and Terrorism: Towards an Urban Geopolitics*. Malden, MA: Blackwell, 2004.

Graham, Stephen and Simon Marvin. *Splintering Urbanism: Networked Infrastructures, Technological Motilities, and the Urban Condition*. New York: Routledge, 2001.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Granovetter, Mark, and Patrick McGuire. "The Making of an Industry." In *Laws of the Markets*, edited by Michel Callon, 147–173. New York: Blackwell, 1998.

Green, Gary, Michael R. Lemov, Cheryl Polydor, Mary Masulla, and Stephen Mallinger. *Investigation of the Health Effects of Irradiated Mail*. Report of the General Counsel of the Office of Compliance, U.S. Congress, OSH-0201,0202. Washington, DC, 2002.

Greenpeace International. *Annual Report*. Multiple vols. Amsterdam: Greenpeace International, 1994–2009. http://www.greenpeace.org/international/en/about/reports/.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Holt, 2014.

Griffin, James M., and Steven L. Puller. "Introduction: A Primer on Electricity and the Economics of Deregulation." In *Electricity Deregulation: Choices and Challenges*, edited by James M. Griffin and Steven L. Puller, 1–30. Chicago: Chicago University Press, 2005.

Haigh, Thomas, Mark Priestley, and Crispin Rope. *ENIAC in Action: Making and Remaking the Modern Computer*. Cambridge, MA: MIT Press, 2018.

Harding, Luke. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. New York: Vintage, 2014.

Harlow, Alvin F. *Old Post Bags: The Story of the Sending of a Letter in Ancient and Modern Times*. New York: Appleton, 1928.

Heal, Geoffrey, Michael Kearns, Paul Kleindorfer, and Howard Kunreuther. "Interdependent Security in Interconnected Networks." In *Seeds of Disaster*, edited by Auerswald et al., 258–276.

Heath, Lee. "Weapons of Mass Disruption." Presentation to Mailers' Technical Advisory Committee, Washington, DC, May 7, 2003. https://ribbs.usps.gov/mtac/documents/tech_guides/.

Henderson, Donald. "The Looming Threat of Bioterrorism." *Science* 283, no. 5406 (1999): 1279–1282.

Henkin, David M. *The Postal Age: The Emergence of Modern Communications in Nineteenth-Century America*. Chicago: University of Chicago Press, 2007.

Herr, Trey, and Ryan Ellis. "Disrupting Malware Markets." In *Cyber Insecurity: Navigating the Perils of the Next Information Age*, edited by Richard Harrison and Trey Herr, 105–122. New York: Rowman & Littlefield, 2016.

Higgs, Robert. *Crisis and Leviathan: Critical Episodes in the Growth of American Government*. New York: Oxford University Press, 1987.

Hilton, George W. "The Consistency of the Interstate Commerce Act." *Journal of Law and Economics* 9 (1966): 87–113.

Hilton, George W. *The Transportation Act of 1958: A Decade of Experience*. Bloomington: Indiana University Press, 1969.

Hirschman, Albert O. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. Cambridge, MA: Harvard University Press, 1970.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Hirsh, Richard F. "Emergence of Electrical Utilities in America." *Powering the Past: A Look Back*. Smithsonian Institution. Last modified September 2002. http://americanhistory.si.edu/powering/past/h1main.htm.

Hirsh, Richard F. *Power Loss: The Origins of Deregulation and Restructuring in the American Electric Utility System*. Cambridge, MA: MIT Press, 1999.

Hirsh, Richard F. "Restructuring or Deregulation?" *Understanding Deregulation*. Smithsonian Institution. Last modified June 2012. http://americanhistory.si.edu/powering/dereg/dereg1a.htm.

Hirsh, Richard F. *Technology and Transformation in the American Electric Utility Industry*. New York: Cambridge University Press, 1989.

Hommels, Anique, Jessica Mesman, and Wiebe E. Bijker, eds. *Vulnerability in Technological Cultures: New Directions in Research and Governance*. Cambridge, MA: MIT Press, 2014.

Hoogenboom, Ari, and Olive Hoogenboom. *A History of the ICC: From Panacea to Palliative*. New York: Norton, 1976.

Horwitz, Robert B. *The Irony of Regulatory Reform: The Deregulation of American Telecommunications*. New York: Oxford University Press, 1989.

Hughes, Thomas P. "The Evolution of Large Technological Systems." In *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, edited by Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, 45–76. Anniversary edition. Cambridge, MA: MIT Press, 2012.

Hughes, Thomas P. *Networks of Power: Electrification in Western Society, 1880–1930*. 1983. Reprint, Baltimore: Johns Hopkins University Press, 1993.

Hughes, Thomas P. "Technology and Public Policy: The Failure of Giant Power." *Proceedings of the IEEE* 64, no. 9 (1976): 1361–1371.

Huntington, Samuel P. "The Marasmus of the ICC: The Commission, the Railroads, and the Public Interest." *Yale Law Journal* 61, no. 4 (1952): 467–509.

Hwang, Ming-Jeng, and Patrick C. Mann. "Deregulation and Efficiency in the Rail Industry." *Atlantic Economic Journal* 15, no. 2 (1987): 47–52.

Idaho National Laboratory. *National SCADA Test Bed Substation Automation Evaluation Report*. Idaho Falls: Idaho National Engineering and Environmental Laboratory, 2009. https://inldigitallibrary.inl.gov/sites/sti/sti/4374057.pdf.

Inglesby, Thomas V. "Anthrax: A Possible Case History." *Emerging Infectious Diseases* 5, no. 4 (1999): 556–560.

Inglesby, Thomas V., Donald A. Henderson, John G. Bartlett, Michael S. Ascher, Edward Eitzen, Arthur M. Friedlander, Jerome Hauer et al. "Anthrax as a Biological Weapon: Medical and Public Health Management." *Journal of the American Medical Association* 281, no. 18 (1999): 1735–1745.

Inglesby, Thomas V., Tara O'Toole, Donald A. Henderson, John G. Bartlett, Michael S. Ascher, Edward Eitzen, Arthur M. Friedlander et al. "Anthrax as a Biological Weapon, 2002: Updated Recommendations for Management." *Journal of the American Medical Association* 287, no. 17 (2002): 2236–2252.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Intelligent Document Task Force. *The Internet of Things: The Final Report of the Intelligent Document Task Force*. Washington, DC: United States Postal Service, 2004.

Intelligent Document Task Force. *Pursuing the Intelligent Document: A Review of Technologies Impacting the Future of Mail, Phase II Report*. Washington, DC: United States Postal Service, 2001.

Intelligent Document Task Force. *Pursuing the Intelligent Document: A Vision for Paper-Based Communications in the Information Age: Phase I Report*. Washington, DC: United States Postal Service, 1999.

ISO/RTO Council. *2009 State of the Markets Report*. Washington, DC, 2009. http://www.isorto.org/Documents/Report/2009IRCStateOfTheMarketsReport.pdf.

ISO/RTO Council. *2010 ISO/RTO Metrics Report*. Washington, DC, 2010. http://www.isorto.org/Documents/Report/2010IRCMetricsReport_2005-2009.pdf.

Jasanoff, Sheila. "Vulnerability and Development—Bhopal's Lasting Legacy." In Hommels, Mesman, and Bijker, *Vulnerability in Technological Cultures*, 89–108.

John, Richard R. "Private Mail Delivery in the United States during the Nineteenth Century: A Sketch." *Business and Economic History* 2, no. 15 (1986): 135–147.

John, Richard R. *Spreading the News: The American Postal System from Franklin to Morse*. Cambridge, MA: Harvard University Press, 1998.

Joskow, Paul L. "Deregulation and Regulatory Reform in the US Electric Power Sector." In *Deregulation of Network Industries: What's Next?*, edited by Sam Peltzman and Clifford Winston, 113–188. Washington, DC: Brookings Institution, 2000.

Joskow, Paul L. "The Difficult Transition to Competitive Energy Markets." In *Electricity Deregulation: Choices and Challenges*, edited by Griffin and Puller, chapter 1.

Joskow, Paul L. "Restructuring, Competition and Regulatory Reform in the U.S. Electricity Sector." In *Designing Competitive Electricity Markets*, edited by Chao Hung-Po and Hillard G. Huntington, 11–31. Boston: Kluwer, 1998.

Joyce, Herbert. *The History of the Post Office: From Its Establishment down to 1836*. London: Bentley & Son, 1893.

Judt, Tony. *Ill Fares the Land*. New York: Penguin, 2010.

Kahn, Alfred. "The Role and Definition of Competition: Natural Monopoly." In *The Economics of Regulation: Principles and Institutions*. Vol. 2, *Institutional Issues*. New York: Wiley and Sons, 1971.

Kaplan, Eben. *Rail Security and the Terrorist Threat*. New York: Council on Foreign Relations, 2007. http://www.cfr.org/united-states/rail-security-terrorist-threat/p12800.

Keeler, Theodore E. *Railroads, Freight, and Public Policy*. Washington, DC: Brookings Institution, 1983.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Kennedy, Jane. "United States Postal Rates, 1845–1951." PhD diss., Columbia University, 1955.

Kielbowicz, Richard B. "A History of Mail Classification and Its Underlying Policies and Purposes." Prepared for the Postal Rate Commission's Mail Reclassification Proceeding, MC95–1. Washington, DC, 1995. http://www.prc.gov/Docs/40/40518/PRC-LR-2.pdf.

Kielbowicz, Richard B. *News in the Mail: The Press, Post Office, and Public Information, 1700–1860s*. New York: Greenwood, 1989.

Kielbowicz, Richard B. *Postal Enterprise: Post Office Innovations with Congressional Constraints, 1789–1970*. Prepared for the Postal Rate Commission. Seattle, WA, 2000. www.prc.gov/tsp/55/enterprise.pdf.

Klein, Naomi. *Shock Doctrine: The Rise of Disaster Capitalism*. New York: Metropolitan/Holt, 2007.

Knight, Frank. *Risk, Uncertainty, and Profit*. New York: Kelley & Millman, 1957. First published 1921 by Hart, Schaffner & Marx.

Kolko, Gabriel. *Railroads and Regulation, 1877–1916*. Princeton, NJ: Princeton University Press, 1965.

Kournikakis, B., S. J. Armour, C. A. Boulet, M. Spence, and B. Parsons. *Risk Assessment of Anthrax Threat Letters*. DRES TR-2001–048. Suffield, Alberta: Defence Research Establishment Suffield, 2001.

Kriebel, Wesley R., and C. Phillip Baumel. "Issues in Freight Transportation Regulation." *American Journal of Agricultural Economics* 61, no. 5 (1979): 1003–1009.

Lakoff, Andrew. "From Population to Vital System: National Security and the Changing Object of Public Health." In *Biosecurity Interventions: Global Health and Security in Question*, edited by Andrew Lakoff and Stephen Collier, 33–60. New York: Columbia University Press, 2008.

Lakoff, Andrew. "Preparing for the Next Emergency." *Public Culture* 19, no. 2 (2007): 247–271.

Lakoff, Andrew. *Unprepared: Global Health in a Time of Emergency*. Oakland: University of California Press, 2017.

Lakoff, Andrew, and Eric Klinenberg. "Of Risk and Pork: Urban Security and the Politics of Objectivity." *Theory and Society* 39, no. 5 (2010): 503–525.

Landau, Susan. *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA: MIT Press, 2013.

Lash, Scott, and Brian Wynne. "Introduction." In Beck, *Risk Society*, 1–8.

Laurits R. Christensen Associates. *Description of the U.S. Freight Rail Industry*. Vol. 1, *Analysis of Competition, Capacity, and Service Quality*. Prepared for the Surface Transportation Board. Washington, DC, November 2009.

Le Dantec, Christopher A., and Carl DiSalvo. "Infrastructure and the Formation of Publics in Participatory Design." *Social Studies of Science* 43 no. 2 (2013): 241–264.

Lester, Elizabeth, Gregory Bearman, and Adrian Ponce. "A Second Generation Anthrax Smoke Detector: An Inexpensive Front-End Monitor That Detects

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Bacterial Spores." *IEEE Engineering in Medicine and Biology* 23, no. 1 (2004): 130–135.

Levin, Richard C. "Regulation, Barriers to Exit, and the Investment Behavior of Railroads." In *Studies of Economic Regulation*, edited by Gary Fromm, 181–230. Cambridge, MA: MIT Press, 1981.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: Wiley & Sons, 2006.

Lin, Herb. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (2012): 46–70.

Lockheed Martin. "Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense." https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Lovins, Amory B., and L. Hunter Lovins. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House, 1982.

Lowenstein, Anthony. *Disaster Capitalism: Making a Killing out of Catastrophe*. New York: Verso, 2015.

Luke, T. W. "Everyday Techniques as Extraordinary Threats: Urban Technostructures and Non-places in Terrorist Actions." In *Cities, War, and Terrorism*, edited by Stephen Graham, 120–136.

Lupton, Deborah. *Risk*. New York: Routledge, 1999.

Lyon, David. *Surveillance after September 11*. Malden, MA: Polity, 2003.

Mailers' Technical Advisory Committee. *MTAC Charter*. Washington, DC: United States Postal Service, 2013. http://ribbs.usps.gov/mtac/documents/tech_guides/mtac_charter.pdf.

Mailing Industry Task Force. *Promote Development of Intelligent Mail*. Washington, DC: United States Postal Service, 2003.

Mailing Industry Task Force. *Seizing Opportunity: The 2001 Report of the Mailing Industry Task Force*. Washington, DC: United States Postal Service, 2001.

Mangold, Tom, and Jeff Goldberg. *Plague Wars: A True Story of Biological Warfare*. New York: St. Martin's, 2000.

Massport. "Security Information." n.d. http://www.massport.com/logan-airport/at-the-airport/security-information.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. New York: Cambridge University Press, 2018.

Maurer, William A. "The Transportation of Hazardous Materials after September 11: Issues and Developments." *Federalist Society for Law and Public Policy Studies*. December 1, 2003. https://fedsoc.org/commentary/publications/the-transportation-of-hazardous-materials-after-september-11-issues-and-developments.

McChesney, Chris. "Toxic Trains: Chemical Transportation Regulation, Terrorism, and the U.S. Capitol." *Sustainable Development Law & Policy* 6, no. 3 (2006): 30–32, 81.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

McDonald, Forrest. "Samuel Insull and the Movement for State Utility Regulatory Commissions." *Business History Review* 32, no. 3 (1958): 241–254.

Miller, Robert H. *Power System Operation*. New York: McGraw-Hill, 1983.

Mindell, David A. *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore: Johns Hopkins University Press, 2002.

Meeks, James E. "Concentration in the Electric Power Industry: The Impact of Antitrust Policy." *Columbia Law Review* 72, no. 1 (1972): 64–130.

Meyer, John, Merton Peck, John Stenson, and Charles Zwick. *The Economics of Competition in the Transportation Industries*. Harvard Economic Studies. Cambridge, MA: Harvard University Press, 1959.

Monahan, Torin. "Questioning Surveillance and Security." In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 1–26. New York: Routledge, 2006.

Moore, Elizabeth A. "Federalism vs. Terrorism: Damaging DC's Defense against Chemical Attacks in *CSX Transportation, Inc. v. Williams*." *George Washington Law Review* 74 (2005–2006): 771.

Morrill, C. D., and J. A. Blake. "A Computer for Economic Scheduling and Control of Power Systems." *Transactions of the American Institute of Electrical Engineers* 74, no. 3 (1955): 1136–1142.

Moteff, John D. *Critical Infrastructures: Background and Early Implementation of PDD-63*. Prepared by the Congressional Research Service. Washington, DC: Library of Congress, 2001.

Moteff, John D. *Critical Infrastructures: Background, Policy, and Implementation*. Prepared by the Congressional Research Service. Washington, DC: Library of Congress, 2003.

Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. New York: Free Press, 2006.

Mustafa, Husain. *Postal Technology and Management*. Mt. Airy, MD: Lomond Systems, 1971.

Nachenberg, Carey. "A Forensic Dissection of Stuxnet." Presented at the Center for International Security and Cooperation, Stanford University, April 23, 2012.

Nagel, Theodore J. "Operation of a Major Electric Utility Today." *Science* 201, no. 4360 (1978): 985–993.

National Commission of Terrorist Attacks upon the United States. "Executive Summary." In *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United Sates*. Washington, DC: Government Printing Office, 2004. http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

National Energy Policy Development Group. *National Energy Policy*. Washington, DC: Government Printing Office, 2001.

National Institute for Occupational Safety and Health. *NIOSH Health Hazard Evaluation Report: HETA #2002-0136-2880, United States Senate and House of*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Representatives, Washington, DC. Cincinnati: Department of Health and Human Services, 2002.

National Science and Technology Council. *Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations*. Washington, DC, 2008. https://fas.org/irp/eprint/biometrics.pdf.

National Security Strategy of the United States. Washington, DC: Government Printing Office, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

National Transportation Safety Board. "CSXT Petroleum Crude Oil Derailment and Hazardous Materials Release." *Railroad Accident Brief*. March 2, 2016.

Nelson, James C. "The Effects of Entry Control in Surface Transport." In *Transportation Economics*, edited by National Bureau of Economic Research, 381–422. New York: Columbia University Press, 1965.

Nelson, James C. *Railroad Transportation and Public Policy*. Washington, DC: Brookings Institute, 1959.

North American Electric Reliability Corporation. *Long-Term Reliability Assessment: 2009–2018*. Princeton, NJ: North American Electric Reliability, 2009.

Nye, David. *Electrifying America: Social Meanings of a New Technology, 1880–1940*. Cambridge, MA: MIT Press, 1997.

O'Brien, Lawrence F. "Lawrence F. O'Brien Oral History Interview XXI." Interview by Michael L. Gillette, LBJ Library, June 18, 1987. http://www.lbjlibrary.net/assets/documents/archives/oral_histories/obrien_l/OBRIEN21.PDF.

O'Brien, Lawrence F. *No Final Victories: A Life in Politics from John F. Kennedy to Watergate*. New York: Doubleday, 1974.

Office of Electricity Delivery and Energy Reliability. *Large Power Transformers and the U.S. Electric Grid*. Washington, DC: Department of Energy, 2012. https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

Office of Electricity Delivery and Energy Reliability. *National SCADA Test Bed Program: Multi-Year Plan, 2008–2013*. Washington, DC: Department of Energy, 2008. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_OE_NSTB_Multi-Year_Plan.pdf.

Office of Electricity Delivery and Energy Reliability. *United States Electrical Industry Primer*. Washington, DC: Department of Energy, 2015. https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.

Owens, Larry. "Vannevar Bush and the Differential Analyzer: The Text and Context of an Early Computer." *Technology and Culture* 27, no. 1 (1986): 63–95.

Paolino, Ross. C. "All Aboard! Making the Case for a Comprehensive Rerouting Policy to Reduce the Vulnerability of Hazardous Railcargoes to Terrorist Attack." *Military Law Review* 193 (2007): 144–177.

Perrow, Charles. *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*. Princeton, NJ: Princeton University Press, 2007.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. 1984. Reprint, Princeton, NJ: Princeton University Press, 1999.

Perrow, Charles. *Organizing America: Wealth, Power, and the Origins of Corporate Capitalism*. Princeton, NJ: Princeton University Press, 2002.

Perrow, Charles. "Shrink the Targets." *IEEE Spectrum* 43, no. 9 (2006): 46–49.

Pierson, Paul. *Politics in Time: History, Institutions, and Social Analysis*. Princeton, NJ: Princeton University Press, 2004.

Pile, James C., John D. Malone, Edward M. Eitzen, and Arthur M. Friedlander. "Anthrax as a Potential Biowarfare Agent." *Archive of Internal Medicine* 158, no. 5 (1998): 429–434.

Plant, Jeremy F. "Terrorism and the Railroads: Redefining Security in the Wake of 9/11." *Journal of Policy Research* 21, no. 3 (2004): 293–297.

Polanyi, Karl. *The Great Transformation*. Boston: Beacon Press, 1944.

Posner, Richard. *Catastrophe: Risk and Response*. New York: Oxford University Press, 2005.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. Washington, DC: Government Printing Office, 1997.

President's Commission on Postal Organization. *Towards Postal Excellence: Report of the General Contractor*. Annex contractor's reports. 4 vols. Washington, DC: Government Printing Office, 1968.

President's Commission on Postal Organization. *Towards Postal Excellence: The Report of the President's Commission on Postal Organization*. Washington, DC: Government Printing Office, 1968.

President's Commission on the United States Postal Service. *Embracing the Future: Making the Tough Choices to Preserve Universal Service*. Washington, DC: Government Printing Office, 2003.

Priest, George L. "The History of the Postal Monopoly in the United States." *Journal of Law and Economics* 18, no. 1 (1975): 34–38.

Public Citizen. *Homeland Unsecured: The Bush Administration's Hostility to Regulation and Ties to Industry Leave America Vulnerable*. Washington, DC: Public Citizen, 2004. https://www.citizen.org/sites/default/files/acf1b7.pdf.

Relyea, Harold C., and Henry B. Hogue. *Department of Homeland Security Reorganization: The 2SR Initiative*. Prepared by the Congressional Research Service. Washington, DC: Library of Congress, 2006. https://www.hsdl.org/?view&did=467158.

Rhodes, Richard. *The Twilight of the Bombs: Recent Challenges, New Dangers, and the Prospect for a World without Nuclear Weapons*. New York: Knopf, 2010.

Ridge, Tom. "Remarks by Secretary Tom Ridge to National League of Cities." Transcript. March 10, 2003. Washington, DC: Department of Homeland Security. https://www.hsdl.org/?abstract&did=475516.

Robin, Corey. *Fear: History of a Political Idea*. New York: Oxford University Press, 2004.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Rodrigue, Jean-Paul, Claude Comtois, and Brian Slack. *The Geography of Transport Systems*. New York: Routledge, 2009. http://people.hofstra.edu/geotrans/index.html.

Rolston, Bri. *Improving Control System Security through the Evaluation of Current Trends in Computer Security Research*. Idaho Falls: Idaho National Engineering and Environmental Laboratory, 2005. https://inldigitallibrary.inl.gov/sites/sti/sti/3395023.pdf.

Rowan, Jim. "Mail Security Task Force Update." Presentation to the Mailers' Technical Advisory Committee. Washington, DC, February 2002.

Rowan, Jim. "Mail Security Task Force Update." Presentation to the Mailers' Technical Advisory Committee. Washington, DC, May 2002.

Saltzstein, Robert, and Ronald Resh. "Postal Reform: Some Legal and Practical Considerations." *William and Mary Law Review* 12, no. 4 (1971): 766–786.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown, 2012.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown, 2018.

Savage, Charlie. *Power Wars: Inside Obama's Post-9/11 Presidency*. New York: Little, Brown, 2015.

Savage, Charlie. *Takeover: The Return of the Imperial Presidency*. New York: Back Bay Books, 2007.

Schewe, Phillip F. *The Grid: A Journey through the Heart of Our Electrified World*. Washington, DC: Joseph Henry Press, 2007.

Schlesinger, Arthur, Jr. *Crisis of the Old Order, 1919–1933*. Boston: Houghton Mifflin, 1957.

Schneier, Bruce. "Beyond Security Theater." *Schneier on Security*. November 2009. https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html.

Schneier, Bruce. "In Praise of Security Theater." *Schneier on Security*. January 2007. https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html.

Schneier, Bruce. "The NSA Is Hoarding Vulnerabilities." *Schneier on Security*. August 2016. https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

Schudson, Michael. *The Rise of the Right to Know: Politics and the Culture of Transparency, 1945–1975*. Cambridge, MA: Belknap Press of Harvard University Press, 2015.

"Section 11(b) of the Holding Company Act: Fifteen Years in Retrospect." *Yale Law Journal* 59, no. 6 (1950): 1088–1119.

Skocpol, Theda. *Diminished Democracy: From Membership to Management in American Civic Life*. Norman: University of Oklahoma Press, 2003.

Spero, Sterling D. *The Labor Movement in a Government Industry: A Study of Employee Organization in the Postal Service*. New York: Arno, 1971.

Spraggins, H. Barry, John Ozment, and Phillip Fanchon. "Risk Modeling of Hazardous Materials Rail Movement to Include a Terrorist Incident." *Journal of the Academy of Business and Economics* 5, no. 3 (2005).

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Star, Susan Leigh. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43, no. 3 (1999): 377–391.

Starr, Paul. *The Creation of the Media: Political Origins of Modern Communications*. New York: Basic, 2004.

Stevens, Nye. *Postal Service Financial Problems and Stakeholder Proposals*. Prepared by the Congressional Research Service, RL31069. Washington, DC: Library of Congress, 2002.

Stone, Richard. *The Interstate Commerce Commission and the Railroad Industry: A History of Regulatory Policy*. New York: Praeger, 1991.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*. Special publication 800–882. Gaithersburg, MD: National Institute of Standards and Technology, 2008.

Sunstein, Cass. *Worst-Case Scenarios*. Cambridge, MA: Harvard University Press, 2007.

Sweeney, James L. *The California Energy Crisis*. Stanford, CA: Hoover Institution, 2002.

Swidler, Ann. "Culture in Action: Symbols and Strategies." *American Sociology Review* 51 (1986): 273–286.

Symantec. *W32.Stuxnet Dossier*. Version 1.4. February 2011.

Tarbell, Ida M. *The History of the Standard Oil Company*. New York: McClure, Philips, 1904.

Terman, Fredrick E. "A Brief History of Electrical Engineering Education." *Proceedings of the IEEE* 86, no. 8 (1998): 1792–1800. Classic paper, reprinted from *Proceedings of the IEEE* 64, no. 9 (1976): 1399–1406.

Teshale, Eyasu H., John A. Painter, Gregory A. Burr, Paul S. Mead, Scott V. Wright, Larry F. Cseh, Ronald Zabrocki et al. "Environmental Sampling for Spores of *Bacillus anthracis*." *Emerging Infectious Diseases* 8, no. 10 (2002): 1083–1087.

Tierney, John T. *Postal Reorganization: Managing the Public's Business*. Boston: Auburn, 1981.

Tierney, John T. *The U.S. Postal Service: Status and Prospects of a Public Enterprise*. Boston: Auburn, 1988.

Transportation Research Board. *Cooperative Research for Hazardous Materials Training: Defining the Need, Converging on Solutions—Special Report 283*. Washington, DC: National Academies Press, 2005. doi:10.17226/11198.

Transportation Safety Board of Canada. "Runaway and Main-Track Derailment: Montreal, Maine & Atlantic Railway Freight train MMA-002 Mile 0.23, Sherbrooke Subdivision Lac-Mégantic, Quebec 06 July 2013." *Railway Investigation Report*, R13D0054. Quebec: Gatineau: Minister of Public Works and Government Services, August 20, 2014.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Tympas, Aristotle. "From Digital to Analog and Back: The Ideology of Intelligent Machines in the History of the Electric Analyzer, 1870s–1960s." *IEEE Annals of the History of Computing* 18, no. 4 (1996): 42–48.

Tympas, Aristotle. "Perpetually Laborious: Computing Electric Power Transmission before the Electric Computer." *International Review of Social History* 48 (2003): 73–95.

United States Postal Service. *2001 Comprehensive Statement on Postal Operations*. Washington, DC, 2001.

United States Postal Service. *2005 Comprehensive Statement on Postal Operations*. Washington, DC, 2005.

United States Postal Service. *2006 Comprehensive Statement on Postal Operations*. Washington, DC, 2006.

United State Postal Service. "Emergency Response to Mail Allegedly Containing Anthrax." Management Instruction EL-860-1999-3. Washington, DC, October 4, 1999.

United States Postal Service. *The Private Express Statutes and Their Administration*. Washington, DC: Government Printing Office, 1973.

United States Postal Service. "Rates for Domestic Letters, 1863–2009." Washington, DC, 2009. http://www.usps.com/postalhistory/_pdf/DomesticLetterRates1863-2009.pdf.

United States Postal Service. *Report on Universal Service and the Postal Monopoly*. Washington, DC, 2008. http://www.usps.com/postallaw/_pdf/USPSUSOReport.pdf.

United States Postal Service. *Response to the House Subcommittee on Transportation, Treasury, Housing and Urban Development, the Judiciary, District of Columbia and the Senate Subcommittee on Transportation, Treasury, Judiciary, Housing and Urban Development, Committees on Appropriations*. Washington, DC, 2006.

United States Postal Service. *United States Postal Service: An American History, 1775–2006*. Washington, DC, 2007. https://web.archive.org/web/20090508205717/http://www.usps.com/cpim/ftp/pubs/pub100.pdf.

United States Postal Service. *United States Postal Service Transformation Plan*. Washington, DC, 2002.

United States Postal Service. *Update on Biohazard Detection System in Response to OIG Report #DA-MA-02–001*. Washington, DC, 2004.

United States Postal Service. *US Postal Service Emergency Preparedness Plan for Protecting Postal Employees and Postal Customers from Exposure to Biohazardous Material and for Ensuring Mail Security against Bioterror Attacks*. Washington, DC, 2002.

United States Postal Service Delivery Support Headquarters. *How to Succeed with MSP*. Washington, DC: United States Postal Service, 2002.

United States Postal Service Engineering. "Decision Analysis Report: Biohazard Detection Systems." Washington, DC, 2004.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

United States Postal Service Office of Inspector General. *Audit Report—Biohazard Detection System Consumables*. DA-AR-06-006. Washington, DC, 2006.

United States Postal Service Office of Inspector General. *Audit Report—Postal Service Strategy for Processing At-Risk Mail and Deployment of Irradiation Equipment*. AC-AR-02-003. Washington, DC, 2002.

United States Postal Service Office of Inspector General. *Biohazard Detection System*. DA-MA-02-001. Washington, DC, 2002.

United States Postal Service Office of Inspector General. "Fact-Finding Review of Actions and Decisions by Postal Service Management at the South Jersey Processing and Distribution Center." LH-MA-02–004. Bellmawr, NJ, 2002.

United States Postal Service Office of Inspector General. *Postal Service's Efforts to Implement Prevention and Detection Technology*. DA-AR-02-008. Washington, DC, 2002.

United States Post Office Department. *Annual Report of the Postmaster General, 1969*. Washington, DC: Government Printing Office, 1970.

United States Post Office Department. *Postal Progress: An Accounting of Stewardship*. Publication 28. Washington, DC: Government Printing Office, 1968.

United States Post Office Department. *Report of the Superintendent of Railway Mail Service*. In *Annual Report of the Post-Master General of the United States for the Fiscal Year Ended June 30, 1878*. Washington, DC: Government Printing Office, 1878.

United States Post Office Department Office of Research and Engineering. *The Post Office: Challenge to Industry*. Publication 48. Washington, DC: Government Printing Office, 1967.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004.

U.S.-Canada Power System Outage Task Force. *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, November 2003.

U.S. Census Bureau. *Commodity Transportation Survey*, *Economic Census*. Washington, DC: Government Printing Office, 1963, 1967, 1972, 1977.

U.S. Census Bureau. *Statistical Abstract of the United States, 2004–2005*. Washington, DC: Government Printing Office, 2005.

U.S. Commission on National Security/21st Century. *Road Map for National Security: Imperative for Change*. Phase III report. Washington, DC, 2001.

U.S. Commission on Postal Service. *Report of the Commission on Postal Service*. Washington, DC: Government Printing Office, 1977.

U.S. Department of Commerce. *The Postal Crisis: The Postal Function as a Communications Service*. Washington, DC: Government Printing Office, 1977.

U.S. Department of Energy. "Enabling Modernization of the Electric Power System." In *Quadrennial Technology Review: An Assessment of Energy Technologies and Research Opportunities*. Washington, DC, 2015. http://energy.gov/sites/prod/files/2015/09/f26/Quadrennial-Technology-Review-2015_0.pdf.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

U.S. Department of Homeland Security. *Budget in Brief: Fiscal Year 2005*. Washington, DC, 2005. https://www.dhs.gov/sites/default/files/publications/FY_2005_BIB_4.pdf, 13.

U.S. Department of Homeland Security. *Privacy Impact Assessment Update for the Enhanced Cybersecurity Services (ECS)*. November 20, 2015. https://www.dhs.gov/sites/default/files/publications/privacy-pia-28-a-nppd-ecs-november2015.pdf.

U.S. Department of Homeland Security. *Privacy Impact Assessment Update for TSA Advanced Imaging Technology*. December 18, 2015. https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf.

U.S. Department of Transportation. *1993 Economic Census*. Washington, DC, 1996.

U.S. Department of Transportation. *Commodity Flow Survey, Economic Census: Transportation*. Washington, DC, 1993–2016. http://www.bts.gov/publications/commodity_flow_survey/.

U.S. Energy Information Administration. *Annual Energy Review*. Washington, DC: Department of Energy, 2017. https://www.eia.gov/totalenergy/data/annual/.

U.S. Energy Information Administration. *Electric Power Annual 2009*. Washington, DC: Department of Energy, 2011. https://www.eia.gov/electricity/annual/archive/03482009.pdf.

U.S. Energy Information Administration. *Electric Power Annual 2017*. Washington, DC: Department of Energy, 2018. https://www.eia.gov/electricity/annual/pdf/epa.pdf.

U.S. Energy Information Administration. *Monthly Energy Review*. Washington, DC: Department of Energy, 2017. https://www.eia.gov/totalenergy/data/monthly.

U.S. Energy Information Administration. *Public Utility Holding Company Act of 1935: 1935–1992*. Washington, DC: Department of Energy, 1993. https://www.eia.gov/electricity/archive/0563.pdf.

U.S. General Accounting Office. *Bioterrorism: Public Health Response to Anthrax Incidents of 2001*. GAO-04-152. Washington, DC, 2003.

U.S. General Accounting Office. *Changes in Electricity-Related R&D*. GAO/RCED-96-203. Washington, DC, 1996. https://www.eia.gov/electricity/annual/archive/03482009.pdf.

U.S. General Accounting Office. *Combating Terrorism: Linking Threats to Strategies and Resources*. GAO/T-NSIAD-00-218. Washington, DC, 2000.

U.S. General Accounting Office. *Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives*. GAO/T-NSIAD-99-112. Washington, DC, 1999.

U.S. General Accounting Office. *Conversion to Automated Mail Processing Should Continue; Nine Digit Zip Code Should Be Adopted if Conditions Are Met*. GAO/GGD-83-24. Washington, DC, 1983.

U.S. General Accounting Office. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. GAO-04-354. Washington, DC, 2004.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

U.S. General Accounting Office. *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*. GAO-02-474. Washington, DC, 2002.

U.S. General Accounting Office. *Energy Task Force: Process Used to Develop the National Energy Policy*, GAO-03-894. Washington, DC, 2003.

U.S. General Accounting Office. *Highlights of GAO's Conference on Options to Enhance Mail Security and Postal Operations*. GAO-02-315SP. Washington, DC, 2001.

U.S. General Accounting Office. *Postal Service: Automation Is Restraining but Not Reducing Costs: GGD-92–58*. Washington, DC, 1992.

U.S. General Accounting Office. *Postal Service: Automation Is Taking Longer and Producing Less than Expected*. GAO/GGD-93-89BR. Washington, DC, 1997.

U.S. General Accounting Office. *Postal Service: Information on the Change to Multiline Readers for the Zip+4 Program*. GAO/GGD-8862BR. Washington, DC, 1986.

U.S. General Accounting Office. *Postal Service: Planned Benefits of Iowa Automated Mail Facility Not Realized*. GAO/GGD-94-78. Washington, DC, 1994.

U.S. General Accounting Office. *Railroad Regulation: Economic and Financial Impact of Staggers Rail Act of 1980*. GAO/RCED-90-80. Washington, DC, 1990.

U.S. General Accounting Office. *US Postal Service: A Primer on Postal Worksharing*. GAO-03-927. Washington, DC, 2003.

U.S. Government Accountability Office. *Anthrax Detection: Agencies Need to Validate Sampling Activities in Order to Increase Confidence in Negative Results*. GAO-05-251. Washington, DC, 2005.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*. GAO-08-119T. Washington, DC, 2007.

U.S. Government Accountability Office. *Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance*. GAO-08-987. Washington, DC, 2008.

U.S. General Accountability Office. *United States Postal Service: Information on the Irradiation of Federal Mail in the Washington, DC, Area*. Briefing to the House and Senate Appropriations Committees. GAO-08-938R. Washington, DC, 2008.

U.S. Government Accountability Office. *US Postal Service: Better Guidance Needed to Ensure Appropriate Response to Anthrax Contamination*. GAO-04-239. Washington, DC, 2004.

U.S. Government Accountability Office. *US Postal Service: Intelligent Mail Benefits May Not Be Achieved if Key Risks Are Not Addressed*. GAO-09-599. Washington, DC, 2009.

U.S. Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC, 2002. https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

U.S. Office of Management and Budget. "Appendix: Homeland Security Mission Funding by Agency and Budget Account." *Analytic Perspectives: Budget of*

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

the U.S. Government, Fiscal Year 2017. Washington, DC: Government Printing Office, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2017/assets/homeland_supp.pdf.

U.S. Office of Technology Assessment. *Implications of Electronic Mail and Message Systems for the US Postal Service*. OTA-CIT-184. Washington, DC: Office of Technology Assessment, 1982.

U.S. Office of Technology Assessment. *Proliferation of Weapons of Mass Destruction: Assessing the Risk*. OTA-ISC-559. Washington, DC: Government Printing Office, 1993.

U.S. Office of Technology Assessment. *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity*. OTA-BP-CIT-12. Washington, DC: Office of Technology Assessment, 1982.

U.S. Office of Technology Assessment. *Transportation of Hazardous Materials*. OTA-SET-304. Washington, DC: Government Printing Office, 1986.

U.S. Postal Inspection Service. *2002 Annual Report of Investigations of the United States Postal Inspection Service*. Washington, DC, 2002. https://postalinspectors.uspis.gov/pressroom/pubs.aspx.

Vietor, Richard H. K. *Contrived Competition: Regulation and Deregulation in America*. Cambridge, MA: Belknap Press of Harvard University Press, 1994.

Vina, Stephen R. *Homeland Security: Scope of the Secretary's Reorganization Authority*. Prepared by the Congressional Research Service. Washington, DC: Library of Congress, 2005. https://fas.org/sgp/crs/homesec/RS21450.pdf.

Wasik, John F. *The Merchant of Power: Sam Insull, Thomas Edison, and the Creation of the Modern Metropolis*. New York: Palgrave Macmillan, 2006.

Weaver, Nicholas. "NSA and the No Good, Very Bad Monday." *Lawfare*. August 16, 2016. https://www.lawfareblog.com/very-bad-monday-nsa-0.

Weick, Karl E. "Normal Accident Theory as Frame, Link, and Provocation." *Organization and Environment* 17, no. 1 (2004): 27–31.

Weik, Martin H. *A Fourth Survey of Domestic Electronic Digital Computing Systems*. Ballistic Research Laboratories report no. 1227. Washington, DC: Department of Commerce, 1964, 89. http://ed-thelen.org/comp-hist/BRL64.html#TOC.

Weszkalnys, Gisa. "Anticipating Oil: The Temporal Politics of a Disaster Yet to Come." Supplement. *Sociological Review* 62, no. S1 (2014): 211–235.

Wilcox, Richard H., and Patrick J. Garrity, eds. *A Nation of Vulnerabilities: Crisis Management in a Society of Networks*. Washington, DC: Center for Strategic and International Studies, Georgetown University, 1984.

Winner, Langdon. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press, 1989.

World Health Organization. *Health Aspects of Chemical and Biological Weapons*. Geneva: World Health Organization, 1970.

Zajtchuk, Russ, and David Franz. "Biological Terrorism." In *Terrorism: Reducing Vulnerabilities and Improving Responses*, by Committee on Counterterrorism

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Challenges for Russia and the United States, 214–221. Washington, DC: National Academies Press, 2004.

Zittrain, Johnathan. *The Future of the Internet—and How to Stop It*. New Haven, CT: Yale University Press, 2008.

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Index

AAR. *See* Association of American Railroads (AAR)
Abraham, Spencer, 214, 216
Acceptance of risk, 232–233. *See also* Critical Infrastructure Protection (CIP) reliability standards
Accidents. *See* Normal accident theory
Accountability, public, 5–8, 10–13, 24, 26, 35, 77, 89, 95, 142, 156, 167, 184, 202, 210–213, 236–237, 240–242, 246–247, 255n37
Acxiom, 182
Advanced Facer Canceller System (AFCS) machines, 177–178
Advanced imaging technology (AIT), 3
ADVO, 182
AEIC. *See* Association of Edison Illuminating Companies (AEIC)
AFCS. *See* Advanced Facer Canceller System (AFCS) machines
AGC. *See* Automatic generation control (AGC)
Airline security, 3
AIT. *See* Advanced imaging technology (AIT)
Al-Hayat, 215
Al-Qaeda, 193, 215. *See also* September 11 attacks, infrastructural changes following
American Chemistry Council, 197
American Express, 182
American Petroleum Institute, 213
American Postal Workers Union (APWU), 171, 179, 281n49
American Public Power Association, 212
American Railway Association (ARA), 190
America's Hidden Vulnerabilities (CSIS), 147
Anacom, 81
Anthrax attacks, 5, 25, 165–166. *See also* Postal security
  Biohazard Detection System, 25–26, 166, 175–179, 241
  cross-contamination of mail, 169–171, 173, 178, 180, 183, 306n32
  forms of infection, 304n2
  Intelligent Mail, 179–183
  likely source of, 304n8
  limitations of CDC-USPS guidelines for, 169–170
  pre-attack planning failures, 167–169
  risk and infrastructure publics, 171–174
  sanitation technologies, 174–176
Appropriations, postal service, 43, 51–55, 96, 262n71, 279n33. *See also* Postal rates
APUM. *See* Association of Public Utility Mailers (APUM)
APWU. *See* American Postal Workers Union (APWU)
ARA. *See* American Railway Association (ARA)
Aradau, Claudia, 10

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Assistant postmasters general, 42
Association for Postal Commerce, 172
Association of American Railroads (AAR), 150, 185
  historical hazardous materials regulation by, 189–191
  post-9/11 response, 191–193
Association of Edison Illuminating Companies (AEIC), 71
Association of Public Utility Mailers (APUM), 96, 281n49
Association of Third Class Mailers, 97
AT&T, 3, 92, 100
Attributable costs, 96, 280n44. *See also* Postal deregulation
Aurilio, Anna, 222
Automated mail processing. *See also* Centralization
  history of, 46–48, 260n47
  postal deregulation and, 101–104
  Sectional Center System, 260n51
  vulnerabilities in, 169–170
  zip codes introduced in, 260n51
Automatic generation control (AGC), 83. *See also* Computer systems, development and use within electric power
Averch-Johnson effect, 274n205
Aviation and Transportation Security Act (2001), 192

B&O railroad, 195
Bacillus anthracis. *See* Anthrax attacks
Bar code sorter (BCS) machines, 102
BDS. *See* Biohazard Detection System
Beame, Abraham, 31
Beck, Ulrich, 14, 21, 23, 25, 156–160, 170, 302n111, 303n131, 303n140. *See also* Risk society
Biden, Joe, 185, 187
Biohazard Detection System (BDS), 25–26, 166, 175–179, 241. *See also* Postal security
Blount, Winton, 92–93, 277n2
Board of Governors (postal service), 94–98, 279n34
Boris, Jay, 114, 187
Bowker, Geoffrey, 15
British Petroleum, 222
Brunton, Finn, 18
Bureaucratization of risk, 24, 163, 206, 247
Bureau of Explosives, 189–190
Bureau of Export Administration, 2, 151
Burger, Warren E., 18
Burrus, William, 171, 179
Bush, George W., 122, 151–152, 162, 172, 185, 189, 206, 213, 297n11, 314n54
  Department of Homeland Security created by, 153–155
  Energy Policy Act passed under, 221–227
  infrastructure security prioritized by, 2–4, 141–145, 163, 246
  Office of Homeland Security created by, 2
  response to 2003 New York blackout, 210, 214–215
  U.S.-Canada Power System Outage Task Force under, 214–221
Bush, Vannevar, 81, 274n211, 275n213
Business and Defense Services Administration, 146
Buzan, Barry, 161

Cabinet Committee to Combat Terrorism, 146–147
California Independent System Operator (CAISO), 128
California Institute of Technology, 81
Capital Exclusion Zone
  creation of, 197
  legal challenges to, 197–202
Capital One, 182
Carey, James, 161
Carter, Jimmy, 110, 119, 282n53
CDC. *See* Centers for Disease Control and Prevention (CDC)
Census Bureau, *Commodity Transportation Survey*, 66
Center for Strategic and International Studies (CSIS), 147

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Centers for Disease Control and Prevention (CDC), 169
Central Hudson Gas & Electric Corp., 32
Centralization. *See also* Distributed control; Normal accident theory
centralized systems, 22, 38
of electrical power industry, 70, 73–76, 116, 124–128, 135, 269n146
of mail processing, 45–46, 48, 91, 101–106, 166, 169–170, 184, 243
Chemical Security Act (2001), 192
Chemical shipments. *See* Hazardous materials shipments
Cheney, Dick, 213, 217–218, 222
Chicago Edison Company, 70
Chrétien, Jean, 214, 216
CIP. *See* Critical Infrastructure Protection (CIP) reliability standards
Citizen Kane (Welles), 70
Citizens Committee for Postal Reform, 87, 92, 277n2
Clapper, James, 1, 249
Clean Air Act (1963), 118
Clerks, postal. *See* Postal workers
Clinton, William, 147–148, 150, 151
Cogeneration, 71–72, 119–121, 290n163
Cohen, Julie A., 74
Cohen, William, 151
Collier, Stephen, 145
Colocation, complexity resulting from, 37–38, 68. *See also* Complex systems; Normal accident theory
COMET. *See* Committee for Efficient Transportation (COMET)
Committee for Efficient Transportation (COMET), 109
Committee Urging Regulatory Reform for Efficient National Transportation (CURRENT), 109
Commodity Transportation Survey, 66
Common-carrier obligations, 60–62, 73, 85, 108, 112, 188, 265nn99–100, 311n11, 311n13. *See also* Railroad regulation
Common-mode components, 36–37. *See also* Complex systems; Normal accident theory;
Complex systems. *See also* Colocation, complexity resulting from; Normal accident theory; spatial dependency
common-mode components, reliance on, 36–37
proximity in, 37–38
Computer systems, development and use within electric power, 69, 81–84, 128, 129, 131, 132, 209, 210, 215, 216, 219, 241, 243, 274n208, 275n213. *See also* Control systems
Connecticut Light & Power Co., 32
Consolidated Edison (Con Ed), 31–32, 74
Consolidated Freightways, 55
Consolidated Rail Corporation (Conrail), 111
Constellation Energy Group, 222
Control systems, 69, 82–84, 124, 128–133, 216, 222, 233, 294n205, 296n223, 320n48. *See also* Computer systems, development and use within electric power; Distributed control systems; Supervisory control and data acquisition (SCADA) systems
Corzine, Jon, 192, 193
Cost-of-service pricing, 64, 268n131. *See also* Railroad regulation
Coupling, tight versus loose, 38–39. *See also* Normal accident theory
Court decisions. *See* Landmark cases
Crestline rail accident, 312n18
Critical assets, 228. *See also* Critical Infrastructure Protection (CIP) reliability standards
Critical Cyber Asset Identification standard, 229. *See also* Critical Infrastructure Protection (CIP) reliability standards
Critical cyber assets, 228. *See also* Critical Infrastructure Protection (CIP) reliability standards

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Critical Infrastructure Assurance Office, 2, 151, 154
Critical Infrastructure Protection (CIP) reliability standards
acceptance of risk, 232–233
approval process for, 322n102
critical assets under, 228
Critical Cyber Asset Identification standard in, 229
critical cyber assets in, 228
Electronic Security Perimeter(s) standard, 229
impact of, 241
Incident Reporting and Response Planning standard, 230
origins of, 227–228
penalties for noncompliance, 234–235, 325n151
Personnel and Training standard, 229
Physical Security of Critical Cyber Assets standard, 230
reasonable business judgement in, 229, 231–232
Recovery Plans for Critical Cyber Assets standard, 230
Security Management Control standard, 229
specificity of, 233–234
Systems Security Management standard, 230
success of, 235–236
table of, 230–231
Violation risk factors, 234–235, 325n151
Critical infrastructure protection, politics of. *See also* Regulatory history; September 11 attacks, infrastructural changes following
cultural construction of infrastructure vulnerability, 145–152
disaster capitalism, 7
government spending levels, 2–3, 151, 154–155
historical risk levels, 139–143
historical thinking and, 239–244
implications for future, 247–248
infrastructure publics, 6, 11, 171–174, 245–246, 254n24
new military urbanism, 12
organized interests, 246–247
politics of risk, 155–162
post-9/11 anxiety and infrastructure inversion, 143–145, 162–163
prioritization of infrastructure, 1–5, 11–14, 142–143
public accountability, 6–8, 11, 236–237 (*see also* accountability, public)
reflexive modernization, 14, 246–247
"security theater," 6–7, 240, 242
social relations produced by, 4–5
Critical Infrastructure Protection Act (2001), 144
Critical Infrastructure Working Group, 148
Cross-contamination of mail, 169–171, 173, 178, 180, 183, 306n32. *See also* Anthrax attacks; Postal security
Cross-subsidies
in freight rail industry, 64–65
in postal system, 41–42, 95–98, 280n42
CSIS. *See* Center for Strategic and International Studies
CSX
2014 rail accident, 207
CSX v. Williams, 197–202, 315n74
Washington, DC, rail lines, 195–196, 315n68
CSX v. Williams, 197–202, 315n74
Cuéllar, Mariano-Florentino, vii, 14, 153, 298n27
Culnan, Mary, 150
Cultural construction of infrastructure vulnerability, 145–152. *See also* Critical infrastructure protection, politics of; September 11 attacks, infrastructural changes following
CURRENT. *See* Committee Urging Regulatory Reform for Efficient National Transportation (CURRENT)

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Cyber assets, 228. *See also* Critical Infrastructure Protection (CIP) reliability standards
Cybersecurity. *See also* Electric power regulation
CIP reliability standards, 227–236
control-system architecture and, 131–133
Energy Policy Act (2005), 221–227
infrastructure as target, 27, 249–252
National Energy Policy Development Group, 213–214, 217–218, 222
NERC consensus language for, 212–214, 220–221
NERC Urgent Action Standard 1200, 221
overview of, 5, 26, 210–211
public accountability and security, 236–237
state-sponsored hacking, 251–252
terrorist threats and, 215–220
U.S.-Canada Power System Outage Task Force, 214–221
"Cyber weapons," 251

Danner, Mark, 11–12
Daschle, Tom, 169
Daystrom computers, 83. *See also* Computer systems, development and use within electric power
DC City Council, 195–197
DCS. *See* Distributed control systems
Defense Threat Reduction Agency, 144
Demand fluctuations
estimation of, 80
Insull's analysis of, 269n147
load factor, 269n148
Department of Commerce, 2
Department of Homeland Security (DHS)
creation of, 2, 153–155, 193
reorganizations of, 300n95
Department of the Interior. *See* Super Power plan
Department of Transportation (DOT), regulatory authority of. *See* Hazardous materials shipments
Deregulation. *See also* Electric power deregulation; Postal deregulation; Railroad deregulation
goals of, 86–90
infrastructure vulnerability arising from, 8–11, 88–90, 133–135, 243–244
overview of, 8–11, 23–25
Detroit, Toledo & Ironton R. Co. Control (DT&I Conditions), 63, 287n119
Dhaliwal, Herb, 214, 216
DHS. *See* Department of Homeland Security (DHS)
Dickens, Charles, 139
Differential analyzers, 81, 275n213. *See also* Computer systems, development and use within electric power
Direct Marketing Association, 172
Disaster capitalism, 7
Distributed control. *See also* Normal accident theory
characteristics of, 38
of electrical power industry, 116
of postal system, 40–41
risk and, 84
Distributed control systems (DCS), 294n205. *See also* Computer systems, development and use within electric power; Control systems
Doyle Report, 287n109
DT&I conditions. *See Detroit, Toledo & Ironton R. Co. Control* (DT&I Conditions)
Duffy, James, 283n57
Duke Energy, 213

Early Bird power system, 81. *See also* Computer systems, development and use within electric power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

E-COM (electronic computer originated mail)
failure of, 99–100
mail volume handled by, 283n59
rates for, 283n60
support for, 282n53
The Economics of Competition in the Transportation Industries (Meyer), 109
EDF. *See* Environmental Defense Foundation (EDF)
Edison, Thomas, 70, 269n146
Edison Electric Institute, 212
Edwards, Paul, 4, 15
EFT. *See* Electronic funds transfer
EIS. *See* Epidemic Intelligence Service (EIS)
Electricity Consumers Resource Council (ELCON), 122, 212
Electric power deregulation
consolidation and centralization of control, 124–128
control systems and, 128–133
driving forces behind, 115–116
Energy Policy Act (1992), 120–124, 292n187
independent power generation, rise of, 119–120
infrastructure vulnerability arising from, 115–116, 133–135
oil crisis and emergence of environmentalism, 117–119, 290n152, 290n159
overview of, 8–9
postwar status quo and, 116–117
Public Utility Regulatory Policies Act (1978), 89–90
technological stasis and, 117–118
Electric power regulation. *See also* Electric power deregulation
electric power as sociotechnical systems, 15–17
federal regulation, 73–78
grow-and-build strategy, 117, 289n140, 289n147
holding companies, 75–76, 271n178, 272n179, 272n186, 273n175
impact of, 68–69, 84
information and communication technologies (ICTs), 78–84, 273n203, 274n208, 275n213
loose coupling, preservation of, 73
monopolies and, 69–70
network interconnection during WWI, 73–74, 270n167
New York City blackout (2003) case study, 209–210
overview of, 34
political economy and, 78–79
Public Utility Holding Company Act (1935), 77–78, 116
Public Utility Regulatory Policies Act (1978), 118–122
rate-of-return regulation, 69, 72–73, 80–81, 84, 274n205
regulatory lag, 274n206
state regulation, 69–73, 269n146
Super Power and Giant Power plans, 74–76, 271nn174–175
utility consensus, 116
Electric Reliability Coalition, 291n174
Electric Reliability Council of Texas (ERCOT), 127, 293n192
Electric Reliability Organization (ERO), 220–221, 223
Electrifying America (Nye), 16
Electronic funds transfer (EFT), 99, 282n50
Electronic message systems (EMS), 99, 282n50
Electronic originated mail. *See* E-COM (electronic computer originated mail)
Electronic Security Perimeter(s) standard, 229. *See also* Critical Infrastructure Protection (CIP) reliability standards
Elkins Act (1903), 266n112
Emerging Infectious Diseases (Inglesby), 168
Eminent domain law, 263n87
EMS. *See* Electronic message systems (EMS)
Encryption, 249

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Energy insecurity, 218. *See also* National Energy Plan; *National Energy Policy* (NEPDG)
Energy Policy Act (1992), 120–124, 292n187
Energy Policy Act (2005)
  implementation of, 224–227
  provisions of, 221–224
ENIAC, 81
Enron, 124, 212, 213
Environmental Defense Foundation (EDF), 290n159
Environmental movement. *See also* Hazardous materials shipments
  advocacy for hazmat transportation security, 185–189, 203–205
  coalitions and press action, 195
  impact of, 117–119, 290n159
  overview of, 26
  politics of green security, 206–208
Environmental Protection Agency (EPA), 118, 192
Epidemic Intelligence Service (EIS), 169
ERCOT. *See* Electric Reliability Council of Texas (ERCOT)
ERO. *See* Electric Reliability Organization (ERO)
EternalBlue, 252
EWG. *See* Exempt wholesale generators (EWG)
Executive Order No. 10988, 278n28
Executive Order No. 13010, 148
Exempt wholesale generators (EWG), 122
Exxon Mobile, 213

Falkenrath, Richard, 189
Fear (Robin), 161
Federal Civil Defense Administration, 146, 168
Federal Energy Regulatory Commission (FERC)
  CIP reliability standards, input into, 227–236, 325n153
  Energy Policy Act's restrictions on, 223–224
  NERC (North American Electric Reliability Council and North American Electric Reliability Corporation) and, 213–214
  Order 672, 224–227
  Order 888, 124–125
  Order 889, 124–125
  Order 2000, 124–135
  power of, 210, 220–221, 292n187
  qualifying facilities rates and, 120
Federal Railroad Administration (FRA), 190, 203
Federal Rail Safety Act (1970), 190, 198–201
Federal Trade Commission (FTC), 77
Fellmeth, Robert C., 110
FERC. *See* Federal Energy Regulatory Commission (FERC)
First-class postage rates, 49, 96–98. *See also* Postal rates
FirstEnergy, 132–133, 215, 320n48
5 Percent Case, 267n117. *See also* Rate-of-return regulation
Florida Power & Light, 213
FRA. *See* Federal Railroad Administration (FRA)
Franchises, energy, 71–72, 77, 84, 270n150. *See also* Electric power regulation
Freight rail deregulation. *See* Railroad deregulation
Freight rail regulation. *See* Railroad regulation
Friends of the Earth, 26, 187, 193, 195, 204–205
FTC. *See* Federal Trade Commission (FTC)
The Future of the Internet—and How to Stop It (Zittrain), 129

Galvin, David, 165
Geertz, Clifford, 160
Geiser, K. R., 82
General Electric (GE), 81–82, 274n212
General Post Office, 259n35. *See also* Postal regulation

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Generative systems, 83
Giant Power plan, 74–76, 271nn174–175
Giddens, Anthony, 157
Gingrich, Newt, 151
Glauthier, T. J., 212
Goldman, Ari, 32
Goldsmith, Jack, viii, 255n37
Gorelick, Jamie, 148
Graham, Stephen, 11
Granger movement, 59, 265n100
Graphnet Systems, 100
Great Depression, 77
Greenberg, Andy, 252
Greenpeace, 7
  hazmat policy coalition, 26, 193, 195, 204–205, 208, 314n54
  public protests by, 185–187
Green security. *See* Hazardous materials shipments
Grow-and-build strategy, 117, 289n140, 289n147. *See also* Electric power regulation
Guardian, 249

Hacking, state-sponsored, 251–252
Harris, Bill, 150
Hart, Gary, 151–152
Hart-Rudman Commission, 151–152
Hazardous materials shipments. *See also CSX v.* Williams; Environmental movement; Railroad regulation; Rerouting regulation
  accident rates, 114, 288n132, 312n18
  accountability and infrastructure reordering, 202–203
  commodity flow data for, 288n126, 288n129
  crisis of control facing, 185–189
  Hazardous Materials Transportation Act (1975), 190, 198, 316n99
  Hazardous Materials Transportation Control Act (1970), 190
  historical perspective of, 66–68, 189–191
  HM-232 regulations, 193–195, 316n85
  Homeland Security Act (2002), 193–195
  Implementing Recommendations of the 9/11 Commission Act (2007), 203–205
  politics of, 206–209
  post-9/11 response, 191–193
  protests against, 185–186
  risk coalitions, 195
  Terrorism Prevention in Hazardous Materials Transportation Emergency Act (2005), 195–202
  as terrorist target, 189
  toxic inhalation hazard (TIH) substances, 114–115, 188, 288n131, 312n14
  volume of, 113–114, 185, 187
Hazardous Materials Transportation Act (1975), 190, 198, 316n99
Hazardous Materials Transportation Control Act (1970), 190
Hearst, William Randolph, 70
Heartbleed, 36–37
Heath, Lee, 165
Henderson, Karen LeCraft, 316n99
Hepburn Act (1906), 266n112
Herodotus, 56
Higgs, Robert, 303n141
High-voltage transmission lines, improvements in, 74, 271n170
Hill, Arthur, 146
Hind, Rich, 185
Hirschman, Albert, 285n86
Hirsh, Richard, 19, 116
Historical nature of infrastructure, 19–21
Historical thinking, importance of, 239–242
HM-232 regulations, 193–195, 316n85
Hoecker, James, 214

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Holding companies. *See also* Electric power regulation
benefits of, 272n179
Middle West Utilities Company, 272n186
number of, 271n178, 273n175
operation of, 75–76
Homeland Security Act (2002), 154, 193–195
Home Rule Act (1973), 198
Hoogenboom, Ari, 59
Hoogenboom, Olive, 59
Hoover, Herbert, 75
Hopkinson, John, 269n148
Hughes, Charles Evans, 72
Hughes, Thomas P., 15, 19, 73, 256n46

IAIP. *See* Information Analysis and Infrastructure Protection (IAIP)
IBM, 81
ICC. *See* Interstate Commerce Commission (ICC)
ICTs. *See* Information and communication technologies (ICTs)
Idaho Power, 232
Implementing Recommendations of the 9/11 Commission Act (2007), 203–205
Incident Reporting and Response Planning standard, 230. *See also* Critical Infrastructure Protection (CIP) reliability standards
Independent service operators (ISOs), 16, 124–128, 293n192, 293n195
Industrial dispersal, 146
Information Analysis and Infrastructure Protection (IAIP), 154. *See also* Department of Homeland Security (DHS); Homeland Security Act (2002)
Information and communication technologies (ICTs)
in electrical power industry, 69, 78–84, 86, 116, 128–133, 216, 219, 232, 273n203, 274n208, 275n213 (*see also* computer systems, development and use within electric power)
in postal system, 43, 95, 99–105, 174–183 (*see also* automated mail processing; E-COM [electronic originated mail])
Infrastructural risk. *See* Risk
Infrastructure
definition of, 15
historical nature of, 19–21
relational nature of, 17–19
as sociotechnical systems, 15–17
Infrastructure publics, 6, 11, 13–14, 17, 24–25, 33–34, 40, 42, 57, 59, 61, 85, 88, 90, 102, 106, 113, 134, 140, 162, 167–168, 171–174, 179, 188–189, 197, 206, 211, 236–237, 239–242, 245–248, 252, 254n24 (*see also* infrastructure, relational nature of)
Infrastructure vulnerability
cultural construction of, 145–152
infrastructure as target, 27, 249–252
political origins of, 8–11, 133–135 (*see also* deregulation)
Inglesby, Thomas V., 168
Inherently safer technologies (ISTs), 188
Institutional costs, 280n40. *See also* Postal rates; Postal regulation; Postal deregulation
Insull, Samuel
bankruptcy and trial, 77
demand analysis by, 269n147
holding companies, 75, 272n186
state regulation promoted by, 70–72, 85
steam turbines advanced by, 269n145
Intelligent Mail, 25, 179–183
Interagency Study Group, 147
Intermediate terrorism, 147
Internet service providers (ISPs), 3
Interstate Commerce Act (1887), 60

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Interstate Commerce Commission (ICC), 34
court cases impacting, 266nn111–112
creation of, 57, 60–62
regulation of hazmat transportation, 190
regulatory policy of, 62–66, 190, 266n111, 267n114
Interstate Commerce Commission Termination Act (1995), 198
The Interstate Commerce Omission (Fellmeth), 110
Interstate Natural Gas Association of America, 213
Inverse elastic pricing, 96–97. *See also* Postal deregulation; Postal regulation
Investor-owned utilities (IOUs), 68–69, 76, 116
Irradiation of mail, 174–176. *See also* Postal security
ISOs. *See* Independent system operators (ISOs)
ISPs. *See* Internet service providers (ISPs)
ISTs. *See* Inherently safer technologies (ISTs)

Jackson, Andrew, 278n25
John, Richard, 19, 41, 278n25
Johnson, Hiram, 72
Johnson, Lyndon, 92
J. P Morgan & Co., 76
Judt, Tony, 8

Kappel, Frederick, 92. *See also* Kappel Commission
Kappel Commission, 92, 102, 279n31. *See also* Postal deregulation
Kennedy, John F., 110, 287n109
Kielbowicz, Richard, 278n25
Klein, Naomi, 7, 303n141
Klinenberg, Eric, 145
Knight, Frank, 21–22
Kolko, Gabriel, 110
Koplan, Jeffrey, 170
Kupperman, Robert H., 147

Labor unions, postal
mechanization and automation and, 53, 263n76
percentage of works represented by, 262n75, 278n28
political activism of, 93
push for postal security, 171–174
Lac-Mégantic, Quebec rail accident, 207–208
La Follette, Robert, 72
Lakoff, Andrew, 21–22, 145, 172
Landau, Susan, 326n9
Landis report, 287n109
Landmark cases
CSX v. Williams, 197–202, 315n74
Munn v. Illinois, 60, 85, 265m100
National Association of Greeting Card Publishers, et al. v. United States Postal Service, 280n45
Smyth v. Ames, 266n111
U.S. v. Trans-Missouri, 266n111
Wabash v. Illinois, 60, 197
Large-volume mailers
E-COM (electronic computer originated mail) and, 100
empowerment of, 90–91, 95, 104–105
information revolution and, 98–99
postal politics and, 5–6, 25–26, 95, 102
postal security and, 167, 171–184, 241, 245
Leahy, Patrick, 169
Leeds & Northrup, 81. *See also* Computer systems, development and use within electric power
Legislation
Aviation and Transportation Security Act (2001), 192
Chemical Security Act (2001), 192
Clean Air Act (1963), 118
Critical Infrastructure Protection Act (2001), 144
Elkins Act (1903), 266n112
Energy Policy Act (1992), 120–124, 292n187
Energy Policy Act (2005), 221–227

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Federal Rail Safety Act (1970), 190, 198–201
Hazardous Materials Transportation Act (1975), 190, 198, 316n99
Hazardous Materials Transportation Control Act (1970), 190
Hepburn Act (1906), 266n112
Homeland Security Act (2002), 154, 193–195
Home Rule Act (1973), 198
Implementing Recommendations of the 9/11 Commission Act (2007), 203–205
Interstate Commerce Act (1887), 60
Interstate Commerce Commission Termination Act (1995), 198
Mann-Elkins Act (1910), 266n112
Motor Carriers Act (1935), 65, 108–109
National Environmental Policy Act (1970), 118
Pendleton Act (1883), 278n25
Postal Accountability and Enhancement Act (2006), 281n48
Postal Act (1792), 41, 260n44
Postal Reorganization Act (1970), 88–89, 93–94, 279n29
Private Express Statutes, 42, 95, 260n44
Public Utility Holding Company Act (1935), 73, 77–78, 116, 221, 272n190
Public Utility Regulatory Policies Act (1978), 89–90, 118–122
Railroad Revitalization and Regulatory Reform Act (1976), 89, 111
Regional Rail Revitalization Act (1973), 111
Staggers Rail Act (1980), 89, 111–112
Terrorism Prevention in Hazardous Materials Transportation Emergency Act (2005), 195–202
Transportation Act (1920), 62–63, 267n114, 267n117, 267n120
USA Patriot Act (2001), 144, 153
Lieberman, Joe, 153
Limited-exposure attacks, 168–169
Linear systems, 32–33, 39, 134. *See also* Complex systems; Normal accident theory
  electric power as, 69, 79–84, 128, 132
  failure in, 36–38, 86
  postal system as, 40–41, 43, 45–48, 57
Little Gypsy power station, 82–83. *See also* Computer systems, development and use within electric power
Load balancing, 82–83. *See also* Control systems
Load factor, 269n148
Long Island Lighting Co., 32
Loosely coupled systems. *See also* Normal accident theory
  characteristics of, 38–39
  electrical power as, 68, 73–74, 77, 79
  postal system as, 45, 47–48, 57, 86, 263n82
  railroads as, 63, 67
Louisiana Power and Light, 82–83

Maersk, 252
Mail Advertisers Service Association, 97
Mailers Council, 172
Mailers' Technical Advisory Committee, 173
Mail security. *See* Postal regulation; Postal security
Mail Security Task Force (MSTF), 173–174
Mann-Elkins Act (1910), 266n112
Manual mail processing, 44–45, 261n52. *See also* Postal regulation
Manufactured uncertainties, 302n111
Marsh, Robert, 148, 150
Mass-casualty attacks, 168
Mauer, Tim, 131
Maximum Freight Rate decision, 266n111
MCI, 100

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Mechanized mail processing. *See also* Postal regulation
history of, 46–48, 260n47
postal deregulation and, 101–104
Sectional Center System, 260n51
security vulnerabilities, 169–170
zip codes, 260n51
Merck, 252
Mergers, railroad, 62–63, 267n124
Meyer, John R., 109
Midcontinent ISO, 127
Middle West Utilities Company, 272n186
Midwest Independent System Operator (MISO), 209, 215
Milwaukee Railroad, 109
MLOCRs *See* Multiline OCRs (MLOCRs)
Modernization, dark side of, 157
Modernization, reflexive, 14, 246–247. *See also* Beck, Ulrich
Monahan, Torin, 245, 254n23
Monopoly power
by electric power industry, 69–70, 78–79
by freight rail industry, 59–60
natural monopolies, 269n139
by postal system, 42–43, 260n45
Morton, Thurston, 277n2
Motor Carriers Act (1935), 65, 108–109
MPLSMs. *See* Multiposition letter-sorting machines (MPLSMs)
MSTF. *See* Mail Security Task Force (MSTF)
Mueller, John, 161
Multiline OCRs (MLOCRs), 102
Multiposition letter-sorting machines (MPLSMs), 101
Municipal power systems, 72–73
Munn v. Illinois, 60, 85, 265m100

N-1 Criterion, 218–219
National Association of Greeting Card Producers, 96, 280n45
National Association of Greeting Card Publishers, et al. v. United States Postal Service, 280n45
National Association of Letter Carriers, 7, 262n75, 263n76
National Association of Regulatory Utility Commissioners, 16
National Civic Federation (NCF), 71–72
National Commission on Terrorist Attacks upon the United States, 143
National Electric Light Association (NELA), 71
National Energy Plan, 119
National Energy Policy (NEPDG), 213, 222
National Energy Policy Development Group (NEPDG), 213–214, 217–218, 222
National Environmental Policy Act (1970), 118
National Health Service, 252
National Industrial Transportation League, 197
National Infrastructure Assurance Council, 151
National Pharmaceutical Stockpile, 169
National Protection and Programs Directorate, 300n95
National Security Agency (NSA), 1, 249–250
National Security Resource Board (NSRB), 146
Natural monopolies, 269n139
Naval Research Lab, 187
NCF. *See* National Civic Federation (NCF)
NELA. *See* National Electric Light Association (NELA)
NEPDG. *See* National Energy Policy Development Group (NEPDG)
NERC. *See* North American Electric Reliability Council (NERC)
Network analyzers, 81, 275n213. *See also* Computer systems, development and use within electric power

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

New military urbanism, 11
New York City blackout of 1977, 31–32, 74
New York City blackout of 2003, 214, 319n24
New York Independent System Operator (NYISO), 128
New York Review of Books, 11
New York Times, 32
Niagara Mohawk Power Corp., 32
"Night of Terror" (Lescaze and Egan), 32
9/11 attacks. *See* September 11 attacks, infrastructural changes following
9/11 Commission Act (2007), 203–205
Nixon, Richard, 87, 93, 277n2
Norfolk Southern, 197
Normal accident theory, 21–24, 35–39, 67–68, 105, 209
  complexity in, 36–38
  coupling in, 38–39
  mail processing and, 105–106
  proximity, complexity resulting from, 37–38
  spatial dependency and, 240–241
  suitability for "all hazards" approach, 258n18
North American Electric Reliability Council (also known as North American Electric Reliability Corporation [NERC])
  CIP reliability standards, 227–235
  consensus language, 212–214, 220–221
  relationship with FERC, 224–227
  Urgent Action Standard 1200, 221
Northrop Grumman, 3, 177
NotPetya, 252
NSA. *See* National Security Agency (NSA)
NSRB. *See* National Security Resource Board (NSRB)
Nye, David, 16
NYISO. *See* New York Independent System Operator (NYISO)

OASIS. *See* Open access same-time information system (OASIS)
Obama, Barack, 2, 163
O'Brien, Lawrence, 87, 91–93, 277n2, 279n30
OCRs. *See* Optical character readers (OCRs)
O'Doherty, Kieran, 283n57
Office of Defense Mobilization, 146
Office of Homeland Security, 2, 143–144, 153. *See also* Department of Homeland Security (DHS)
Oil, rail shipments of, 207. *See also* Hazardous materials shipments
Oil crisis (1973), 117–119, 290n152
Open access same-time information system (OASIS), 125
Optical character readers (OCRs), 101–104
Orange & Rockland Utilities, 32
Order 672 (FERC), 224–227
Organized interests, impact of, 246–247
Organized regional markets, 124–127, 292n189
Orum, Paul, 192
Overblown (Mueller), 161

P&DCs. *See* Processing and Distribution Centers (P&DCs). *See also* Postal deregulation
Pacific Gas & Electric (PG&E), 231, 290n159
Path dependency, 19–20
Patriot Act (2001), 144, 153
Patterson, Kathy, 196, 314n56
PCCIP. *See* President's Commission on Critical Infrastructure Protection (PCCIP)
Pearl Street Station, 70, 269n146
"Peek-and-poke" mail processing, 44–45. *See also* Postal regulation
Pendleton Act (1883), 278n25

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Penn Central railroad, 109
Perrow, Charles, vii, 9, 21–23, 35–39, 105, 257n58, 257n72, 258nn17–20, 259n30, 263n82. *See also* Normal accident theory
Personnel and Training standard, 229. *See also* Critical Infrastructure Protection (CIP) reliability standards
Pfaffenberger, Bryan, 18
PG&E. *See* Pacific Gas & Electric (PG&E)
PHMSA. *See* Pipeline and Hazardous Materials Safety Administration (PHMSA)
Physical Security of Critical Cyber Assets standard, 230. *See also* Critical Infrastructure Protection (CIP) reliability standards
Pierson, Paul, 19
Pinchot, Gifford, 75, 76
Pipeline and Hazardous Materials Safety Administration (PHMSA), 203. *See also* Hazardous materials shipments
PJM Interconnection, 215
Policy windows, 302n117
Politics of infrastructure security. *See* Critical infrastructure protection, politics of
Pools. *See* Railroad regulation, pools
Port security, 3–4
Positive train control (PTC), 188
Postal Accountability and Enhancement Act (2006), 281n48
Postal Act (1792), 41, 260n44
Postal deregulation
  appropriations process, 96, 279n33
  Board of Governors, oversight by, 94–98, 279n34
  Citizens Committee for Postal Reform, 87, 92, 277n2
  E-COM (electronic computer originated mail), 99–100, 282n53, 283nn59–60
  ICT strategies in, 98–104
  infrastructure vulnerability arising from, 8–9, 103–104, 133–135
  limitations of, 105–106
  mechanization and automation in, 101–104
  postal rates, 95–98, 278nn25–26, 280n40, 280n44, 281nn46–47
  Postal Reorganization Act (1970), 88–89, 93–94, 279n29
  Private Express Statutes, 95
  push for comprehensive reform and, 90–94
  selective and incomplete nature of, 104–105, 285n86
Postal Rate Commission, 17, 94, 97 100, 279nn37–38, 280nn40–44, 281n46, 282n51, 282n56, 283n60. *See also* Postal rates; Postal Regulatory Commission
Postal rates. *See also* Postal Rate Commission; Postal regulation; Postal Regulatory Commission
  attributable costs and, 280n44
  historical rates, 49, 262n67
  institutional costs and, 280n40
  politics of, 95–98
  reallocation of costs, 281nn46–47
  role of, 278n25, 278nn25–26
Postal regulation. *See also* Postal deregulation; Postal Rate Commission; Postal Regulatory Commission; Postal security; Post Office Department; United States Postal Service (USPS)
  appropriations and expenditures, 51–55, 96, 262n71, 279n33
  capital project funding, 53–55
  Congressional oversight of, 41–43, 49–52
  Cost Ascertainment System, 262n68
  distributed control, and, 40–41
  employment numbers, 45–47
  General Post Office, 259n35
  labor unions, 53, 171–174, 262n75, 263n76, 278n28
  mail volume, 45–46, 261n52, 277n15

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

manual mail processing, 45–46, 261n52. *See also* Postal regulation
mechanization and automation in, 46–48, 260n47, 260n51
monopoly power, 42–43, 260n45
operating deficits, 49–51, 261n61, 261n66
Postal Act (1792), 41, 260n44
postal modernization, 49
postal rates, 49, 261n66, 262n67, 278n25
President's Commission on Postal Organization, 44–45, *55*
Private Express Statutes, 42, *95*, 260n44, 278n23m, 278n27
R&D (research and development) spending, 40, *52–54*, 101
relational infrastructure in, 17–18
Research and Development Bureau, *53*
resilience and, 40–41
structure of, 34, 41–43, *55–57*, 277n17
Postal Regulatory Commission, 17. *See also* Postal Rate Commission
Postal Reorganization Act (1970), 88–89, 93–94, 279n29
Postal security. *See also* Anthrax attacks
Biohazard Detection System (BDS), 176–179
conflicting forces in, *5*
cross-contamination of mail, 169–171, 173, 178, 180, 183, 306n32
historical risk levels, 139–140
large-volume mailers and, 167, 171–184, 241, 245
limitations of CDC-USPS guidelines for, 169–170
overview of, *25–26*, 165–167
politics of, 184
pre-attack planning failures, 167–169
risk and infrastructure publics, 171–174
sanitation technologies, 174–176
total mail visibility, 180
Postal workers
historical employment numbers, 45–47
labor unions, 53, 93, 171–174, 262n75, 263n76, 278n28
manual mail sorting by, 44–*45*
reduction of workforce, 103, 284n76, 284n80
temporary staff, 182–183, 310n85
Postmaster general, 42, 49, 277n22, 279n34
Post Office Department, 34, 40–43, *45*, 48–49, *52–55*, *85*, 87–88, 94, 101–104, 139 *See also* Postal regulation
Potter, John E., 173
Power trusts. *See also* Electric power regulation
holding companies, *75–76*, 271n178, 272n179, 272n186, 273n175
Super Power and Giant Power plans, 74–76, 271nn174–175
Presidential Decision Directive 39, 147–148
Presidential Decision Directive 63, 150–151
Presidential Policy Directive on infrastructure protection (2013), *15*
President's Commission on Critical Infrastructure Protection (PCCIP), 44–45, 147–150
President's Commission on Postal Organization, 44–47, *55*, 261nn60–61, 279n31. *See also* Kappel Commission
Presorting discounts, 281n49
Price-and-entry regulation
in freight rail industry, *57*
in postal system, 32–33
Private Express Statutes, 42, *95*, 260n44. *See also* Postal deregulation; postal regulation
Processing and Distribution Centers (P&DCs), 104, 285n85. *See also* Postal deregulation

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Proximity, complexity resulting from, 37–38. *See also* Complex systems; Normal accident theory; spatial dependency
PTC. *See* Positive train control (PTC)
Public accountability. *See* Accountability, public
Public Interest Research Group, 222
Public Service Electric & Gas Co., 32
Public utility commissions (PUCs), 16. *See also* Electric power deregulation; Electric power regulation; State regulation of electric power
Public Utility Holding Company Act (PUHCA), 73, 77–78, 116, 221, 272n190
Public Utility Regulatory Policies Act (1978), 89–90, 118–122
PUCs. *See* Public utility commissions (PUCs)
PUHCA. *See* Public Utility Holding Company Act (PUHCA)

Qualifying facilities (QFs), 119–120, 290n163, 291n168

Railroad deregulation
  costs of, 113–115
  impact of, 106, 112–113, 287n121
  infrastructure vulnerability arising from, 133–135
  overview of, 8–9
  push for, 106–110, 287n109
  Railroad Revitalization and Regulatory Reform Act (1976), 89, 111
  Regional Rail Revitalization Act (1973), 111
  Staggers Rail Act (1980), 89, 111–112
Railroad regulation. *See also* Hazardous materials shipments; Interstate Commerce Commission (ICC); Railroad deregulation
  abandonments, mergers, and excess track, 62–63, 267n124, 268n127
  charters and state commissions, 60, 265nn99–100
  common-carrier obligations, 85, 188, 311n11, 311n13
  competition, impact of, 108–110, 264nn90–91, 264nn95–97
  durability of, 107–108
  historical risk levels, 139–140
  monopoly power, 59–60
  need for, 59–60
  overview of, 34
  path-dependent processes and, 19–20
  performance under, 266n113
  pools, 60–61, 264n97, 265n98, 266n114
  railroad growth and expansion, 58, 62, 263n87
  rates, 60–66, 267n114, 267nn117–118
  rebates, 60–62, 264n91, 264n96, 265n98, 266n112
  revenue per ton-mile, 264n96
  rise of trucking and, 64–66, 108–109, 263n84
  state support and subsidies, 58, 263nn85–86
Railroad Revitalization and Regulatory Reform Act (1976), 89, 111
Railroads and Regulation (Kolko), 110
Railway Alert Network, 192
Ralph Nader Study Group, 110
Rate-of-return regulation. *See also* 5 Percent Case
  Averch-Johnson effect, 274n205
  ICTs supported by, 69, 84
  initial rational for, 61–62
  rate base calculation in, 80–81
  replaced by functional unbundling, 293n201
  state regulation and, 72–73
Rate regulation. *See also* Postal rates
  electrical power industry, 60, 264n97, 265n98
  freight rail industry, 60–66, 267n114, 267nn117–118
Reasonable business judgement, 229, 231–232. *See also* Critical Infrastructure Protection (CIP) reliability standards

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Rebates, railroad, 60–62, 264n91, 264n96, 265n98, 266n112
Recovery Plans for Critical Cyber Assets standard, 230. *See also* Critical Infrastructure Protection (CIP) reliability standards
Reflexive modernization, 14, 246–247. *See also* Beck, Ulrich
Regional Rail Revitalization Act (1973), 111
Regional transmission organizations (RTOs), 16, 124–128, 293n192, 293n195
Regulatory history, 8–11, 19, 24–25, 75–76. *See also* Cybersecurity regulations; Electric power regulation; Freight rail regulation; Postal regulation
  price-and-entry regulation, 32–33
  resilience generated by regulation, 84–86
Regulatory lag, 274n206
Relational nature of infrastructure, 17–19
Relations of definition, 159
Rerouting regulation
  accountability and infrastructure reordering, 202–203
  coalitions supporting, 195
  Implementing Recommendations of the 9/11 Commission Act (2007), 203–205
  legal challenges to, 197–202
  politics of green security, 206–208
  as referendum on deregulation, 187–189, 206
Research and Development Bureau (Post Office), 53
Research and Special Programs Administration (RSPA), 190
Resilience, 33. *See also* Regulatory history
  normal accident theory and, 22–23, 35–39, 105–106, 258n18
  of postal system, 40–41
  regulation and, 84–86
Ridge, Tom, 143, 216
Risk
  bureaucratization of, 24, 163
  definitions of, 21–22
  historical levels of, 139–140
  normal accident theory of, 22–23, 35–39, 105–106, 258n18
  as policy windows, 302n117
  politics of, 155–162
  post-9/11 anxiety and, 141–143, 162–163
  risk society, 21, 23, 157–160
  uncertainty versus, 21–22, 302n111
Risk, Uncertainty, and Profit (Knight), 21
Risk society, 21, 23, 157–160
Robin, Corey, 161
Rock Island railroad, 109
Roosevelt, Franklin D., 77, 272n190
Routing controls. *See* Rerouting regulation
R. R. Donnelley, 182
RSPA. *See* Research and Special Programs Administration (RSPA)
RTOs. *See* Regional transmission organizations (RTOs)
Rudman, Warren, 151–152
Rural Electric Administration, 272n190

San Diego Gas and Electric, 231
Satcher, David, 170
SCADA systems. *See* Supervisory control and data acquisition (SCADA) systems
Schneier, Bruce, viii, 250
SEC (Securities and Exchange Commission). *See* Securities and Exchange Commission (SEC)
Second-class postage rates, 49, 96–98, 279n39. *See also* Postal rates
Section 11(b), Public Utility Holding Company Act, 78. *See also* Electric power regulation; Public Utility Holding Company Act (1935); State regulation of electric power
Sectional Center System, 260n51. *See also* Postal regulation

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Securities and Exchange Commission (SEC), 78
Securitization, 161–162. *See also* Critical infrastructure protection, politics of
Security Management Control standard, 229. *See also* Critical Infrastructure Protection (CIP) reliability standards
"Security theater," 6–7, 240, 242
September 11 attacks, infrastructural changes following. *See also* Critical infrastructure protection, politics of
  cultural construction of infrastructure vulnerability, 145–152
  Department of Homeland Security (DHS), creation of, 153–155
  hazardous materials shipments, 191–193
  infrastructure publics, 6, 11, 254n24
  new military urbanism, 12
  politics of risk, 155–162
  post-9/11 anxiety, 141–143, 162–163
  prioritization of infrastructure security, 1–5, 11–14, 143–145
  public accountability, 6–8, 11, 236–237 (*see also* accountability, public)
  reflexive modernization, 14
Shadow Brokers, 251
Sherman Antitrust Act, 266n111
Short-run costing methodology, 96–97. *See also* Postal deregulation; Postal rates
Siebel Systems, 182
Sierra Club, 26, 187, 193, 195, 197
Single-area interpretation, 78, 273n194. *See also* Electric power regulation
Single-position letter-sorting machines (SPLSMs), 101
Skocpol, Theda, 278n25
Slammer Worm, 132–133
Smith, William, 171
Smyth v. Ames, 266n111
Snow, John W., 314n54
Snowden, Edward, 249
Sociotechnical systems, 15–17
Southern Pacific Railroad, 111
Spatial dependency, 240–241. *See also* Complex systems; Normal accident theory; Proximity, complexity resulting from
SPLMSs. *See* Single-position letter-sorting machines (SPLMs)
Spoke-and-hub design (postal system), 104, 284n83
Stagflation, 118
Staggers Rail Act (1980), 89, 111–112
Standard Oil, 59, 264n91
Star, Susan Leigh, 15, 256n53
Starr, Paul, 19
State regulation of electric power. *See also* Public utility commissions (PUCs); Regulation of electric power; Section 11(b), Public Utility Holding Company Act
  history of, 32, 69–72, 76, 78, 116, 121, 269n146, 270n157
  models of, 72–73
  state commissions, 60, 265nn99–100
State-sponsored hacking, 251–252
Steam turbines, 269n145
"Still Fun City in Rockaway Peninsula" (Goldman), 32
Stuxnet, 133, 296n223, 327n15
Subsidies, railroad, 58, 263nn85–86
Sullivan, Emmet G., 198
Super Power plan, 74–76, 271nn174–175. *See also* Electric power regulation
Supervisory control and data acquisition (SCADA) systems, 128–129, 216, 294nn204–205. *See also* Computer systems, development and use within electric power; Control systems
Swidler, Ann, 160
Symbol Technologies, 182

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Systems Security Management standard, 230. *See also* Critical Infrastructure Protection (CIP) reliability standards

Tampa Energy and Progress Energy, 231–232
Targets, infrastructure as, 27, 249–252
Telemetry systems, 80, 273n203. *See also* Computer systems, development and use within electric power
Temporary postal workers, 182–183, 310n85
Tennessee Valley Authority, 272n190. *See also* Regulation of electric power
Terrorism Prevention in Hazardous Materials Transportation Emergency Act (2005)
  legal challenges to, 197–202
  passage of, 195–197
Terrorism Risk Analysis and Security Management Plan, 192
Third-class mail postage rates, 96–98. *See also* Postal rates
Thornberry, Mac, 153
Tightly coupled systems. *See also* Normal accident theory
  characteristics of, 22, 38–39, 67, 69
  in electrical power industry, 76, 115–116, 127–128, 210, 227
  postal system as, 48, 91, 99, 104–105
TIH. *See* Toxic inhalation hazard (TIH) substances
Time, 31
Total mail visibility, 180. *See also* Intelligent Mail
Toxic inhalation hazard (TIH) substances. *See also* Hazardous materials shipments
  average rail shipment of, 114–115, 288n131
  definition of, 312n14
  rerouting of, 188 (*see also* rerouting regulation)
Transients, system stability and, 81, 275n213
Transportation Act (1920), 62–63, 267n114, 267n117, 267n120
Transportation Message (Kennedy), 287n109
Transportation Security Administration (TSA), 3, 189, 192
Transportation Worker Identification Credential (TWIC), 3–4
Trucking industry
  hazardous materials, transportation of, 113–114
  rise of, 64–66, 108–109
Trump, Donald, 2, 163
TSA. *See* Transportation Security Administration (TSA)
TWIC. *See* Transportation Worker Identification Credential (TWIC)

Uncertainty, 21–22, 302n111. *See also* Risk
Unionization. *See* Labor unions, postal
United Corporation, 76
United Federation of Postal Clerks, 262n75, 263n76
United States Postal Inspection Service (USPIS), 165
United States Postal Service (USPS). 25, 88, 90, 94–95, 98, 103. *See* Postal deregulation; Postal regulation; Postal security
Urgent Action Standard 1200, 221
USA Patriot Act (2001), 144, 153
U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), 167
U.S.-Canada Power System Outage Task Force
  formation of, 214–215
  prioritization of security and terrorism within, 215–220
  recommendations of, 220–221
  reports and findings, 215
  security defined by, 217–220

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

U.S. Department of Agriculture (USDA), 107
USPS. *See* United States Postal Service (USPS)
U.S. v. Trans-Missouri, 266n111
Utility consensus, 116. *See also* Electric power deregulation; Electric power regulation

Vail, Theodore, 139
Value-of-service pricing, 64, 96, 268n131. *See also* Postal deregulation; Postal rates; Railroad deregulation; Railroad regulation
Verizon, 3, 249
Violation risk factors, 234–235, 325n151. *See also* Critical Infrastructure Protection (CIP) reliability standards

Wabash v. Illinois, 60, 197
Waever, Ole, 161
Wanamaker, John, 278n25
WannaCry, 251–252
"War against terrorism," 6, 141–142
War Industries Board, 74, 270n167
Washington Post, 3
Wasik, John F., 77
Watergate break-in, 88
Webber, Frank, 192
Welles, Orson, 70
Wenner, Seymour, 280n42, 281nn46–47
Westinghouse, 81
Wheeling, 122. *See also* Electric power deregulation
WHO. *See* World Health Organization (WHO)
Wilde, Jaap de, 161
Williams, Anthony, 196. *See also CSX v. Williams*
Wilson, Woodrow, 72
Winner, Langdon, 13
Wiretapping capabilities, 326n9
Working Group on Community-Right-to-Know, 192
World Health Organization (WHO), 168
World War I, interconnected power networks during, 73–74, 270n167. *See also* Electric power regulation
World Wide Threat Assessment, 1
Worms
  NotPetya, 252
  Slammer Worm, 132–133
  Stuxnet, 133, 327n15
  WannaCry, 251–252
Wright, Arthur, 269n148
Wyden, Ron, 249

Xerox, 100

Young & Rubicam, 182

Zero-days, 27, 249
Zip codes, introduction of, 260n51
Zittrain, Johnathan, 129–130

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024

Downloaded from http://direct.mit.edu/books/book-pdf/2368673/book_9780262357777.pdf by guest on 21 November 2024